Key Determinants Influencing Stakeholders' Trust Towards Their Intention to Adopt Smart City Services in Australian Regional Cities

By

Chiranjivi Neupane

Thesis

Submitted in fulfilment of the requirements for the degree of

Master of Informatics

School of Engineering & Technology

Central Queensland University

First submission: 16th December 2019

Re-submission of final version: 11 August 2020

Declarations

Candidate's Statement

By submitting this thesis for formal examination at CQUniversity Australia, I declare that it meets all requirements as outlined in the Research Higher Degree Theses Policy and Procedure.

Statement of Authorship and Originality

By submitting this thesis for formal examination at CQUniversity Australia, I declare that all the research and discussion presented is the original work of the author. No content of this thesis has been submitted or considered, either in whole or in part, at any tertiary institute or university for a degree or any other category of award. I also declare that any material written by another person or institute presented in this thesis has been referenced and listed in the reference section.

Copyright Statement

Previous Submission Statement

This thesis has not been submitted for an award by another research degree candidate (Co-Author), either at CQUniversity or elsewhere.

Acknowledgement of Professional Services

Professional proof-readers, Adrian Taylor and Jonathon Dyer provided copyediting and proof-reading services, according to the guidelines laid out in the University-endorsed national guidelines, 'The editing of research theses by professional editors.'

Declaration of Co-Authorship and Co-Contribution

Paper title: A trust based smart city adoption model for the Australian regional cities: a conceptual framework.

Reference: Neupane C, Wibowo, S, Grandhi, S, and Hossain R 2019, 'A trust based smart city adoption model for the Australian regional cities: a conceptual framework', *Proceedings of the 30th Australasian Conference on Information Systems* (ACIS 2019), 9-11 December, Fremantle, Australia, pp. 420-426.

Status: Published (Conference Proceedings)

Nature of Candidate's Contribution: In conducting the study, I was responsible for writing and presentation in ACIS2019 conference. This publication was written and drafted by me. I formulated the research question, collated the literature, described methodology and concluded the paper. [85%]

My co-authors, Dr. Santoso Wibowo, Dr. Srimannarayan Grandhi and Dr. Rahat Hossain reviewed, edited and supervised the research. [15%]

Chiranjivi Neupane

Date: 16/12/2019

Abstract

Comprised of nearly half the global population, cities are striving to deploy innovative technologies to become ‘smart cities’ and provide technology driven urban solutions. Smart cities are those equipped with numerous Internet of Things (IoT) devices and sensors, interconnected with intelligent information systems where data is generated, communicated and analysed. The benefits of smart cities are numerous, but cyber security is a major concern as smart city infrastructure requires interdependent and uninterrupted operation of multiple technology assisted services. Security issues have always been related to users’ trust on the technology. Literature shows the vital role of trust in innovative technology adoption. There is a need of study on trust-based adoption of smart city services and technologies with security aspects in mind. While there are many studies on the smart city security challenges and solutions in urban settings, this study of regional Australian cities and towns is beneficial to identify trust-determining factors and their influence on stakeholder intention to adopt new technologies and services related to smart cities.

The research framework prepared for the study was tested and assessed using data collected from a questionnaire survey. The data from the sample size of 225 was analysed using IBM SPSS and SmartPLS software. The survey participants were information and communication technology (ICT) professionals working in the central Queensland regions, who were also regarded as important stakeholders for development and adoption of smart cities. Purposive and snowball sampling techniques were applied to gather data from the most eligible respondents. The data analysis process used SmartPLS and IBM SPSS software. Data was analysed using descriptive statistics and Structural Equation Modelling (SEM).

The data analysis assessed nine proposed hypotheses, where four hypotheses were found to be supported by the data and three other hypotheses test results indicated weak positive relationships between the constructs. Perceived usefulness, perceived external pressure and perceived information security were found to be strong positive influencing factors towards stakeholder's trust on smart city services and technologies. Similarly, trust has been found to have a strong positive relationship with intention to adopt smart city services and technologies. The results of this research suggest further studies to explore weak performing relationships found between trust and factors such as information security culture, government policy and perceived privacy. Further research using quantitative as well as qualitative approaches is recommended in order to assess the reasons for the observed significant positive and weak relationships between the factors.

Keywords: Australian smart cities, information security, trust, regional cities, adoption

Acknowledgement

Many people have played vital roles in the successful completion of this study and it is a pleasure to acknowledge the essential motivational, technical, moral and psychological support I received on my research journey. The guidance, expertise and encouragement of others was a constant motivation.

First, I owe a deep sense of thanks and gratitude to my principal supervisor Dr. Santoso Wibowo for believing in me, and always mentoring, motivating and encouraging me to complete my research. I have been greatly influenced by the insight he has in smart cities development.

Second, I feel lucky being under the supervision of my associate supervisors Dr. Srimannarayan Grandhi and Dr. Md Rahat Hossain, who were always there to advise and encourage me. Special thanks to Dr. Grandhi, who provided endless advice, technical support and encouragement throughout.

Third, I would like to thank Dr. Marilyn Wells who supervised my study during the first year of this research. I am also grateful to the School of Graduate Research for providing me partial financial support during the final term of my research candidature.

Finally, I must thank my wife Manju and son Sarvin for being caring and supportive throughout the inevitable ups and downs of my study. For me there was nothing better than watching my son's smile to revitalise me for another day of research. I must also thank my parents for being with me and supporting me physically and emotionally, which always enabled me to progress towards my research goal. Last but not least, special appreciation and

gratitude goes to all the survey participants, who volunteered their precious time to complete the survey questionnaire.

Chiranjivi Neupane

Table of Contents

List of Tables

List of Figures

List of Acronyms

CFA –	Confirmatory Factor Analysis
DoS –	Denial of Service
EFA –	Exploratory Factor Analysis
HOC –	Higher Order Constructs
HOT –	Human Organisation Technology
HTMT -	Heterotrait – Monotrait Ratio of Correlations
ICT –	Information and Communication Technology
IoT –	Internet of Things
KMOSA –	Kaiser-Meyer-Olkin test of Sampling Adequacy
LOC –	Lower Order Constructs
PLS –	Partial Least Square
SEM –	Structural Equation Modelling
TAM –	Technology Acceptance Model
TOE –	Technology Organisation Environment

List of Publication

1. Neupane C, Wibowo, S, Grandhi, S, and Hossain R 2019, 'A trust based smart city adoption model for the Australian regional cities: a conceptual framework', *Proceedings of the 30th Australasian Conference on Information Systems* (ACIS 2019), 9-11 December, Fremantle, Australia, pp. 420-426.

1 Introduction

1.1 Introduction

This chapter contains an overview of research background, statement of problem, significance of the study, aim of the research, objectives and questions, overview of methodology, assumptions made and structure of the thesis chapters. Section 1.2 provides background information about the research problem. Section 1.3 discusses the statement of problem while Section 1.4 discusses the aim, objectives and research questions. Section 1.5 describes the significance of the study and the research methods and assumptions are presented in Section 1.6. Finally, Section 1.7 presents the structure of the thesis with short descriptions about the composition of each chapter.

1.2 Research Background

The global market of smart cities is expected to achieve US$1.565 trillion by 2020, with the majority being in North America and Europe (Frost & Sullivan, 2014). Smart cities are interpreted as an urban hub that is safe, secure, greener, and more efficient as a result of integrated Internet of Things (IoT) devices and networks comprised of databases and artificial intelligent systems (Talari et al., 2017). Advancement in the technology and digital sector has shaped significant changes in human lifestyles. Governments are increasingly utilising innovative technologies to facilitate solutions to urban challenges which are delivering economic, social and environmental benefits. About 70% of the worldwide population is now urban and the urban population is expected to double in the next three decades when compared to two decades ago (Braun et al., 2018). Consequently, smart city solutions have gained popularity and there are strategies and implementation plan in many countries. To address the problems that may arise due to population growth and to improve the living standards of their citizens, local cities are transforming to smart cities (Dewi et al.,

2018). Smart city services use information and communication (ICT) assisted intelligent systems to enhance liveability, workability and sustainability by making urban infrastructure and services more efficient and better integrated (Braun et al., 2018; Dewi et al., 2018).

Yet there are obstacles to the unfettered adoption of smart city technology, not least the growing problem of cybercrime. Data breaches cost the global economy more than $2 trillion by the year 2019 (Juniper Research, 2015) while spending on cyber security in Australia increased 6.5 per cent in 2018 compared to 2017, which totalled to $3.8 billion (Arboleda, 2017). Security of smart city services contributes to this spending because the complex digital infrastructure of smart cities makes them susceptible to cyber-attacks. Elmaghraby and Losavio (2014) and Khatoun and Zeadally (2016) indicate that having a single security risk or vulnerability in a smart city, exploited by a person or an organisation, leads to the entire city being at risk.

Secondly, the security of a smart city can be compromised via its enabling technologies as well as applied management protocols (Gharaibeh et al., 2017). Technologies such as IoT, network infrastructure, and cloud computing have security related issues, where in many cases the security of one technology depends on the security of an interconnected device or system (Elmaghraby & Losavio, 2014). The core of the security in an interconnected system is primarily to protect data generated by humans in their personal life, social life, work life, home life and transport activity. Therefore, security of the smart city is closely related to security of the underlying technology as well as security of information generated by humans interacting with the system.

Further, a number of developed and developing countries have ongoing smart cities plans, while many cities have begun implementing smart citu related projects. Therefore, it is important to be proactive and have security strategies to mitigate future cyber incidents as security breaches may lead to significant negative social, economic and legal impacts. There is, therefore, a need of research to look at various security aspects of smart cities from the planning phase. Many organisations such as KPMG Australia, IoTSec Australia, and Securing Smart Cities are engaged in research and development related to Australian smart cities' security threats and solutions. This indicates that there are current efforts by various organisations towards research in the area of smart city and security and privacy issues related to smart cities. However, most of the existing studies and literature related to smart cities and their security aspects are theoretical. So, there are needs of knowing the perceptions of stakeholders on security and trust issues which may influence their intention to adopt smart city services. Therefore, this research proposed a model for the research and has tested it with the help of survey data. A number of hypotheses were proposed and tested to analyse the relationships between dependent and independent factors.

1.3 Statement of Problem

Literature highlights several deployments of smart city services including smart energy, smart parks, smart precincts, smart lighting, smart transportation, smart water, smart governance, smart tourism, smart security and safety (Dewi et al., 2018; Van Zoonen, 2016). Despite the benefits, there are security challenges that often influence the adoption of smart city services. Almuraqab and Jasimuddin (2017) emphasise that security challenges are a key factor which can negate the adoption of smart cities. This is further supported by Braun et al. (2018) and Dewi et al. (2018) who claim that security related challenges are the major concern for smart cities adoption. The use of innovative and smart technologies for smart city transformation is

essential, but the intention to adopt the available technologies by its stakeholders is more important. Mayer et al. (1995), define trust as the readiness to be vulnerable by the actions of another party. It is identified as a critical component for technology adoption, as it addresses risk, vulnerability and uncertainty (Gefen et al., 2003).

Trust and security are interrelated in the adoption of new technologies as an individual's belief on security may have an influence on their adoption intention (Neupane et al., 2019). In fact, previous studies considered trust as a factor in predicting adoption intention behaviour (Belanche et al., 2012). Although, previous studies (Chourabi, 2012; Dewi et al., 2016; Van Zoonen, 2019) have been conducted on the importance of security and privacy for the adoption of smart cities through the development of a smart city initiative model and security model, these studies were limited to technology, organisational and environmental factors and did not consider security and privacy implications. Literature presents limited evidence on smart cities adoption in Australian cities, let alone the effect of security and privacy on trust in the adoption of smart city services in regional Australia. Based on a report by the Australian Government (2018), many regional cities are experiencing low or negative growth, as jobs lost in the manufacturing sector, or more recently the resources and energy sectors, are not replaced quickly enough. Hence, it is critical for governments to plan for the future of regional cities by maximising their unique advantages and supporting their long-term growth through the development and implementation of smart city services, so the cities can achieve their full potential. This study provides a comprehensive review of important factors that influence stakeholders' trust towards their intention to adopt smart city services in regional Australian cities and, further, develops a conceptual framework by reviewing the models used for studying the users' adoption behaviour towards innovations. This study also explores

the role of security-related factors in influencing stakeholders' trust towards their intention to adopt smart city services.

1.4 Research Aim, Questions and Objectives

The aim of this research is to identify the determining factors on the stakeholders' trust towards their intention to adopt smart city services in regional Australia. The following research questions are set to fulfil the research aim:

RQ1 What are the security challenges for smart cities?

RQ2 What are the determining factors on stakeholders' trust towards their intention to adopt smart city services and technologies in regional Australian cities?

RQ3 What are the recommendations for improving stakeholders' trust towards smart city adoption in regional Australian cities?

To accomplish the research aim, and to answer these research questions, a number of research objectives have been listed. The research objectives outline the tasks that need to be followed during the research process to answer the research questions.

- To identify key cyber security challenges for smart cities.
- To develop a research framework for a trust based smart city adoption model based on review of the literature.
- To identify factors influencing stakeholders' trust towards their intention to adopt smart city services.
- To provide recommendations for future studies to improve stakeholder's trust towards smart city services adoption.

1.5 Significance of the Study

This study provides a comprehensive review of the security threats and vulnerabilities in smart cities and reviews adoption models for innovative technologies to develop a new research model. Stakeholders' trust and their intention to adopt smart city services and technology is a core theme where various factors influencing trust and intention to adopt smart city services are tested by a proposed model. Furthermore, research results indicate a significant influence of trust on stakeholders' intention to adopt smart city services. The result of this study is significant as it explores the trust influencing factors, including information security, that determine stakeholders' intention to adopt smart cities in regional Australia. The findings from this study will trigger further research on the usefulness and intention to transform a current city into a smart city with smart services by considering various factors while designing smart city projects.

1.6 Research Methods and Assumptions

The main aim of the research is to identify the key factors which influence stakeholders' trust towards their intention to accept and adopt smart city services in regional Australian cities. The research considers Technology-Organisation-Environment (TOE) dimensions as a foundation for establishing factors in the model. Also, adding a security dimension to TOE enables the researcher to examine the research problem from security perspectives. So, combining well established theory, widely used in the study of technology adoption and acceptance, with the information security related factors, provides a very good opportunity to test and discuss the findings empirically.

The research was conducted by online survey. This means the research is solely quantitative leading to quantitative data analysis using IBM SPSS version 26.0 (IBM Corp., 2019) and

SmartPLS version 3 (Ringle et al., 2015) for the descriptive analysis and Structural Equation Modelling (SEM) respectively. The research framework was then tested, and results interpreted, based on supported or rejected hypotheses and other statistics.

The regional cities in Queensland are assumed to be the representative area of regional Australia for the sampling purpose. To maintain rigour in the research design, no other significant assumptions have been made.

1.7 Thesis Structure

A total of seven chapters are organised in the thesis, each of which describes the research context, aims and objectives, review of literature, development of research framework, methodology of the research, data analysis and results, conclusion and recommendations for further study. A brief explanation of each chapter is presented below.

Chapter 1: Introduction- This chapter provides a conceptualised description of the research context, problem statement, research aims and objectives and research questions. The significance and background of the research is discussed. In summary, the first chapter represents the overview of the research and thesis.

Chapter 2: Literature Review- In this chapter, the concept of smart city is discussed along with technologies used, associated security challenges, and smart city initiative models.

Chapter 3: Conceptual Framework- This chapter reviews various theoretical models used in technology adoption and trust-based models and proposes a new theoretical framework for the research called ‘trust-based smart city adoption model’. A number of hypotheses have

been developed based on the research framework, which are tested using quantitative data from a survey.

Chapter 4: Research Methodology- This chapter describes the methodology followed by this research study. The use of quantitative method, sampling, data analysis and tools used are explained in this chapter.

Chapter 5: Data Preparation and Analysis- This chapter discusses the data preparation and cleaning process and performs statistical analysis conducted to validate the constructs, structural model, reliability, normality, SEM and path analysis required to assess the hypotheses.

Chapter 6: Hypothesis Testing and Discussion: This chapter presents the major findings of the research study and evaluates how the research questions have been answered with the help of hypothesis test results.

Chapter 7: Conclusions: The final chapter explains the conclusions of the research study and provides suggestions for future research based upon the data analysis and findings. Most importantly, implications, limitations of the current study and suggestions for further research are identified and informed in this section.

2 Literature Review

2.1 Introduction

This chapter explores the literature to conceptualise smart cities, the dimensions, initiatives and information security related challenges associated with smart city services and their related technologies. Section 2.2 presents some definitions of the smart city provided by various authors. Section 2.3 discusses the dimensions and entities of smart cities as discussed by the literature. Various smart city initiative models presented by previous research are reviewed in Section 2.4. Section 2.5 highlights examples of smart cities. Section 2.6 discusses various smart city initiatives in Australian contexts. Section 2.7 discusses security and privacy issues related to smart cities. Finally, Section 2.8 is a summary of the chapter. The summary of Chapter 2 is presented in Figure 2.1 below.

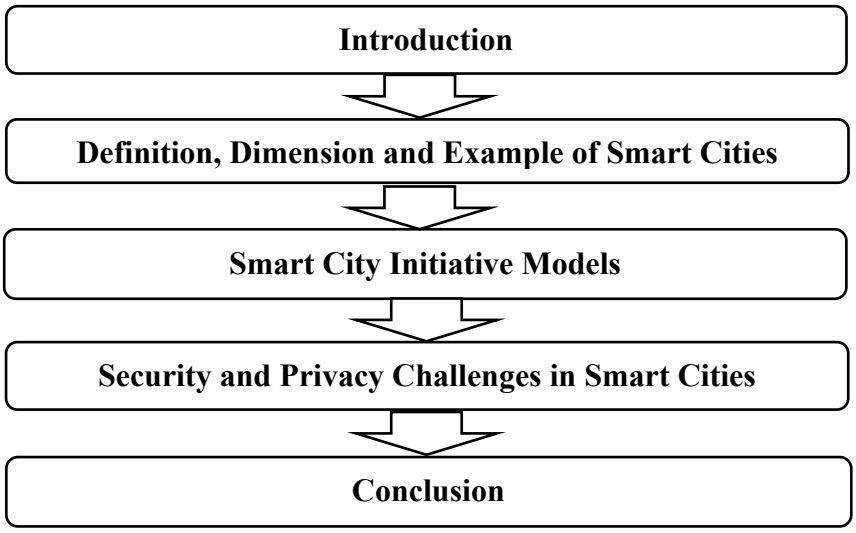


Figure 2.1 Overview of Chapter 2

2.2 Definition of Smart Cities

A basic definition of a smart city is one where ICT assisted infrastructures enable extensive monitoring and guidance towards city maintenance, transport, water and air quality, energy uses, tourist movements and neighbourhood sentiments etc., where a massive amount of data is generated that can be used towards smart management of cities (Van Zoonen, 2016). Smart cities also aim to provide cost effective service delivery to the marginalised part of society (Hayat, 2016). Dubbeldeman and Ward (2015) define a smart city as one which gains sustainable economic growth and good living standards with improved management of natural resources via participatory resources, while all of the above are fuelled by investment in human and social capital, pre-existing infrastructure and innovative technologies. Table 2.1 presents key definitions of smart cities as found in various literature.

The purpose of developing smart cities can be summarised as an effort to create improved daily lives of citizens by integrating technology and innovation. However, the wide scale of data generated and collected in smart cities triggers concern regarding data privacy and security. Therefore, privacy and security related to smart city's devices, networks and applications needs to be explored further.

Table 2.1 Key Definitions of Smart City

Definition	Authors
An innovative and sustainable city which utilises information technology to enhance the efficiency of city services and quality of livings while ensuring necessity of current and upcoming generations are covered in terms of social, environmental and economic aspect	Lea (2017)
A city where conventional networks and services are transformed to more flexible, efficient, and sustainable by the help of information and communication technology (ICT), for the benefit of that city's inhabitants	Mohanty et al. (2016)
A city containing ICT assisted infrastructures enabling extensive monitoring and guidance towards city maintenance, transport, water and air quality, energy uses, tourist movements and neighbourhood sentiments etc., where massive amount of data is generated that can be used towards smart management of cities.	Van Zoonen (2016)
An urban environment supported by ICT systems, which is able to offer innovative and advance services to city inhabitants promoting overall quality of life.	Piro et al. (2014)
A future centric safe, secure, green and efficient urban centre equipped with advanced technological infrastructures such as sensors, electronics interconnected with networks to promote growth in economy and quality of life.	Schaffers et al. (2012)
Smart city is a city with following characteristics: - Proper use of networked infrastructure - Business led urban development - Achieving inclusion in public services - Significant attention on role of social and relational capital in urban development - Have focus on high-tech industries and creative industries - Social and environmental sustainability	Caragliu et al. (2011)

2.3 Dimensions of Smart Cities

There are a number of literature sources that examine smart city initiatives, and many have regarded smart city services as closely related to e-government services and information technology services that are being used towards solving everyday urban problems (AlAawadhi & Morris, 2009; Lombardi et al., 2012; Nam & Pardo, 2011). There is no well-established definition of smart cities and the concept is often associated with its dimensions. The 'smart' prefix on every dimension of a smart city is associated with the network of various devices and services which generate useful data. Different authors such as Bartoli et

al. (2011), Nam and Pardo (2011), Ferraz and Ferraz (2014) and Zhang et al. (2017) present different dimensions that constitute smart cities.

Nam and Pardo (2011) conceptualise smart cities with three dimensions: (a) technology, (b) people, and (c) community. The technology dimension of smart cities involves concepts of digital city, intelligent city, ubiquitous city, wired city, hybrid city and information city. The people dimension involves the concept of creative city, learning city, humane city and knowledge city, whereas the community dimension has the concept of smart community. Figure 2.2 shows Nam and Pardo's (2011) concepts of smart cities within different dimensions.

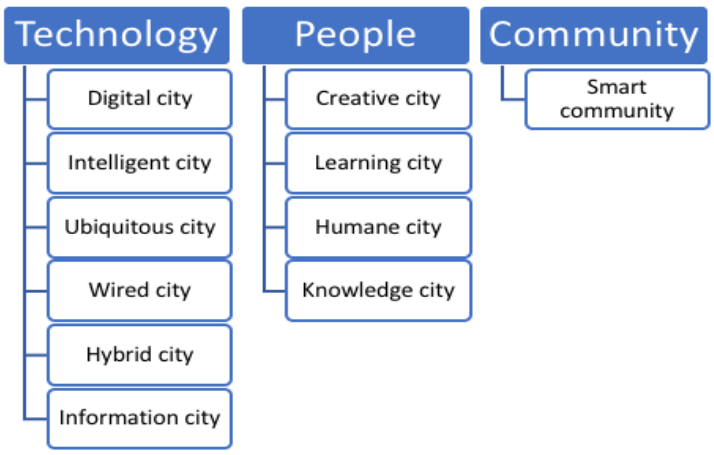


Figure 2.2 Concepts of Smart Cities Within Various Dimensions

Source: Adapted from Nam and Pardo (2011)

Similarly, Bartoli et al. (2011) claim that 'smartness' of the smart cities is provided by three dimensions. They consist of hardware/software dimensions, database dimensions, and management system dimensions. The authors further outline the security related issues that need to be addressed in the smart cities and conclude that smart cities require the highest

level of security and it is necessary to have comprehensive architecture with built-in security from the beginning.

Zhang et al. (2017) categorise smart city architecture into three different dimensions including physical world, communication world and information world. In the physical world, various IoT devices such as wearable devices, environmental sensors and smart sensing devices are connected to the heterogeneous communication channels (networks) such as sensor network, cellular network, ad-hoc network and Wi-Fi networks. The data gathered by the IoTs, stored in cloud and database servers, is processed in the processing units where decisions are made by utilising the data. Similarly, Ferraz and Ferraz (2014) identify main dimensions of the smart cities as related system type, sensors (mechanisms for data gathering from citizen or environment), actuators (way of information returning to users), sensitivity level of information and grouping level by value of information. Table 2.2 shows the classification of smart city components as represented by Ferraz and Ferraz (2014).

Table 2.2 Key Dimensions of Smart Cities

Entity	**Classification**	**Description**
System type	Education Public Safety Transportation Energy and Water Healthcare Government	Concerns to the related system types.
Sensors	Physical Social	Associated with the technique used to gather data from citizen.
Actuators	Direct Indirect	Associated to the method by which information is returned to the user.
Sensitivity Level	Private Public	Associated with the value degree that grouping of information is as needed.

Source: Ferraz and Ferraz (2014)

Lea et al. (2014) represent six key conceptual dimensions of the smart city practices, which are: urban openness, service innovation, partnership formation, urban proactiveness, infrastructure integration and governance. The authors further propose sub-dimensions for each of the dimensions, based on the literature of innovation management cited in the smart city related literature. Most of the dimensions listed by Lea et al. (2014), and presented in Table 2.3, have direct stakeholders' participation or engagement required, which suggests that adoption of these dimensions is a key to the success of smart city. In other words, the relevant party's acceptance of smart city dimensions is likely to lead to the acceptance of smart city.

Table 2.3 Smart City Dimensions and Sub-Dimensions

Dimension	**Sub-dimension**	**Focal point**
Urban Openness	Participatory service design Open data platform availability	Design a mutually acceptable solution
Service innovation	Service diversity Service integration	Unique services involving diversity
Partnership formation	Private-public partnership types Funding resources	Collaboration and resource sharing
Urban proactiveness	Intelligent technology embedded in smart city services Smart green services related to environment and energy	Sustainable services
Smart city infrastructure integration	Multiple device/platform availability City's own network infrastructure Data centre availability and integration	Availability and interoperability
Smart city governance	Smart city leadership Smart city strategy Dedicated organisation for promotion of smart city Smart city development and management processes Smart city principals Performance measurement	Governance structure

Source: Lea et al. (2014)

The points of focus from review of smart city dimensions provided by Lee et al. (2014) have been presented in Table 2.3. It shows that the focus of urban openness can be towards designing a mutually acceptable solution for smart cities. Similarly, service innovation dimension interprets towards unique services with diversity. Further, partnership formation, urban proactiveness and infrastructure integration dimensions focuses on collaboration and resource sharing, sustainable service and availability and interoperability. Finally, the focus of the governance dimension is towards governance structure of the smart city.

Dimensions, entities, indicators and performance indicators related to smart cities are defined in different ways by different authors. Hara et al. (2016) list six dimensions of smart cities as ICT, environmental sustainability, productivity, quality of life, equity and social inclusion and physical infrastructure, where sub-dimensions are represented as smart city entities. Bosch et al. (2017) on the other hand, represent people, planet, prosperity, governance and propagation as the dimensions of the smart cities in their smart city indicator framework. In contrast, Jucevičius et al. (2014) indicate smart city's digital dimensions as innovative, learning, network, knowledge driven and sustainable. Smart city's dimensions presented by different authors represent broad categorisation of the smart city services or entities. The next section briefly describes the main entities of smart cities found in past literature.

Ibrahim et al. (2017) provide a stakeholder engagement model for smart and sustainable cities, which suggest the aspects of stakeholders' involvement in the development of smart cities. The authors indicate local government, private organisations and banks as priority stakeholders while other stakeholders include unions, universities and schools. However, the study was based on the hypothetical activities of the smart city's projects such as reducing local unemployment rate and enhancing healthcare services. This informs towards selection

of an appropriate sample for data collection for the proposed research. The smartness of the smart city largely depends upon the generation of data and effective analysis and communication of data from one system to another system. Table 2.4 summarises the smart city entities presented by various authors.

Table 2.4 Key Entities of Smart Cities

Smart City Entities	**Source**
Environment, economy, society, and satisfaction	Hara et al. (2016)
Economy, environment, energy, people, lifestyle, mobility, technology, and governance	Ojo et al. (2015)
Economy, people, governance, mobility, environment, and living	Lombardi et al., (2012), Giffinger et al. (2007)
Transportation, environment, healthcare, energy, education, safety and other policy domains	Nam and Pardo (2011)

The entities of smart cities found in the various literature in the Table 2.4 and the smart city dimensions presented in Figure 2.2, Table 2.2 and Table 2.3 suggest that there are few dimensions agreed by more than one literature source. For instance, Nam and Pardo (2011) view smart cities within the dimensions of technology, people and community, where Ferraz and Ferraz (2014) classify smart city dimensions in the categories of system types, sensors, actuars and sensitivity level of these technical dimensions. Further, Hara et al. (2016) regard environment, economy, society and satisfaction as entities of smart cities. The literature sources indicate entities and dimensions as a similar term when it comes to understanding smart cities. In a nutshell, smart cities dimensions and entities are mainly related to technology, organisation and organisational environment. Theories for smart city initiatives may further help to identify different factors smart cities are related to.

2.4 Smart City Initiative Models

There are several models that have been developed to understand smart city initiatives and factors that play a role towards their success. The smart city initiative models are also represented as smart city initiative framework or smart city framework. Chourabi et al. (2012) developed an integrative model for the smart city initiative to explain the relationship between various factors. The types of variables used in the initiative model are organisational, technical and contextual and all factors are believed to have a two-way impact towards smart city initiative. The factors differentiated into two levels of impact are: technology, organisation, policy, governance, people communities, economy, natural environment and built infrastructure. Figure 2.3 presents the smart city initiative model developed by Chourabi et al. (2012).

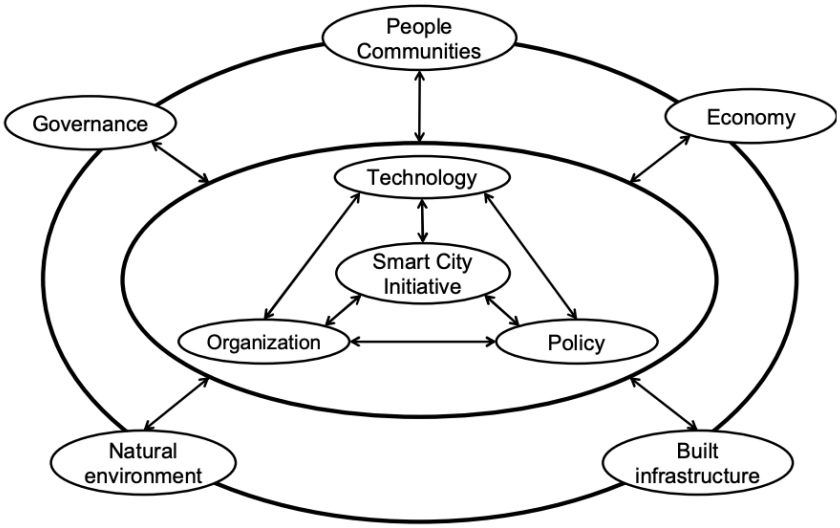


Figure 2.3 Smart City Initiative Model

Source: Chourabi et al. (2012)

Joshi et al. (2016) developed a conceptual model for the smart city initiative where the authors identified and proposed six factors such as technology, economy, legal, social,

management and sustainability that influence the initiatives of smart city. The study provides a good base for identifying the stakeholders in smart cities and the areas that concern cyber security that can be analysed using this model. Figure 2.4 shows the smart city initiative model proposed by Joshi et al. (2016), where security of the smart cities is assumed to be related to factors such as social, technological and management. This model is useful for relating the different factors which impact successful initiation and adoption.

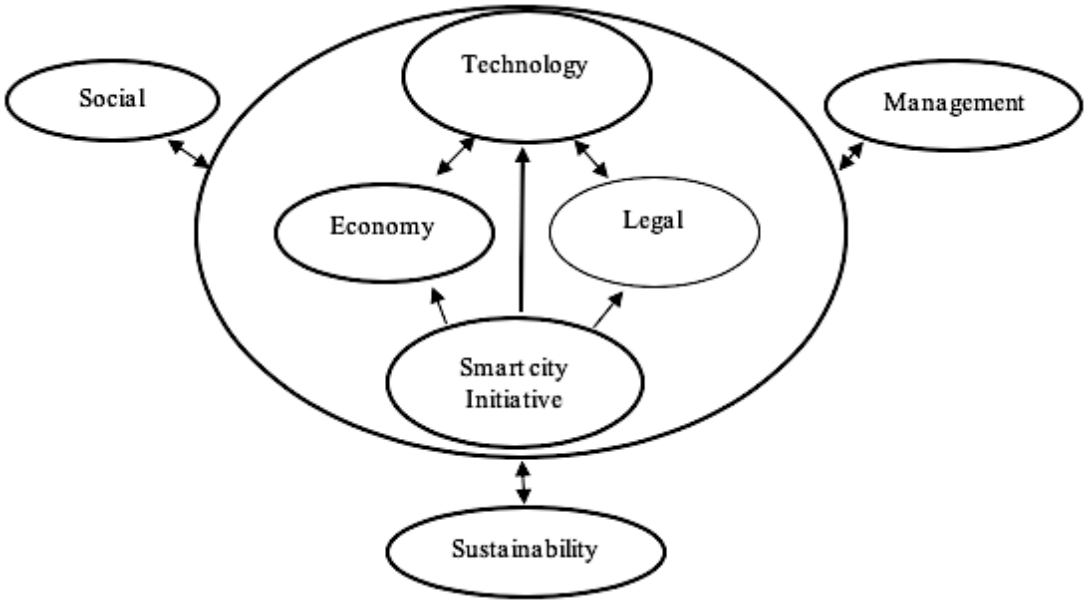


Figure 2.4 Smart City Initiative Model

Source: Joshi et al. (2016)

Smart city initiative models show that there are no well accepted factors and their specific alignment in the model. While Joshi et al. (2016) agree technology and legal or policy related factors as internal factors as outlined by Chourabi et al. (2012), authors present economy as internal factors. So, the factors will not be included as internal and external but within other broad dimensions. Chapter 3 will further discuss the various factors to design the theoretical

framework. Some real-world examples of smart cities will be discussed in the next Section 2.5.

2.5 Examples of Smart Cities

Public and private sectors are investing significantly in smart city technologies (Fishman & Flynn, 2018; Law et al., 2019). To understand real world smart cities, it is best to look at some examples of smart cities projects around the world. Many nations have initiated the implementation of smart cities, some of the examples are briefly discussed in following sections:

Singapore: Having a strong and stable economy, Singapore is moving towards its smart city implementation goal with 100 per cent broadband penetration, smart mobility, smart healthcare and a target of 80%of buildings achieving Green Mark Certification Standards by 2030. There is considerable progress towards smart energy, with at least 30% of houses installed with a smart grid system. In addition, real time public transport information on the internet, and a large proportion of green vehicles, indicates positive progress towards smart mobility (Vidyasekar, 2013).

Barcelona: With the implementation of various innovative attributes of smart cities, Barcelona has a holistic approach towards smart city development. Barcelona has a large domain of services directed towards achieving smart city status. This makes Barcelona stand out among cities that have prioritised various high technical attributes.

San Diego: The streetlights are designed in such a way that they can be remotely tuned to provide light as needed without impacting sensitive areas of the city. The city expects to

achieve more than $250,000 a year in energy savings. Further, parking and other data can be pulled out from the sensors for real time analysis (Vidyasekar, 2013).

Dublin: Dublin is integrating geospatial data with sensors data from across the city to monitor traffic and keep traffic moving. The main smart cities trends in Dublin are mobile and cloud computing, IoT, big data, machine learning and artificial intelligence (Cudden, 2018). Cudden cites some of the examples that Dublin is getting smarter as: intelligent transport system, adaptive signalling in traffic, extensive CCTV camera network, interactive dashboard for data visualisation, carbon neutral stadium equipped with IoT devices, flood monitoring with sensors, and real time weather data. It can be generalised from the example of Dublin that smart city infrastructure involves devices, data and networks all in their advanced and intelligent version.

Santander: The Spanish city of Santander is widely recognised as a smart city largely facilitated by IoT devices and sensors. Both public and private projects have facilitated the smart services including measurement of environmental data such as temperature, humidity, speed and position of vehicles, traffic congestion, public transportation timing and situation, air quality and water network monitoring (Mehmood et al., 2017).

These examples of smart cities around the world indicate there is growing scope and there are expansions of smart city services on the way in many cities. The smart city services adopted include smart grid, smart vehicle, smart healthcare, smart parking, and smart energy optimisation to name but a few. As Australia is the feature of the research, it is vital to understand smart city initiatives in this context. The next section addresses smart city initiatives in an Australian context.

2.6 Smart City Initiatives in Australia

The Australian Government has documented smart cities and suburbs plans, where a significant budget has been allocated to support the delivery of innovative and smart city projects throughout urban and regional areas (Australian Government, 2016). The smart cities plan by the Australian Government involves creating productive, accessible and liveable cities, which can attract talent, boost innovation and generate new jobs and economic growth. The collaborative projects of the Australian smart cities program have the following objectives:

- Use of shared knowledge and expertise towards enhancing capacity and capability of smart cities
- Acquire innovation and talent and broad adoption of smart solutions
- Advancement of standard and improved regulation
- Produce greater outcome via leverage of funding.

The Australian Government smart cities plan indicates that smart cities have three basic pillars: smart investment, smart policy and smart technology. Various projects to accomplish these pillars have been successful in the Round 1 implementation of smart cities in Australia. Table 2.5 shows the key areas and projects of smart cities that were implemented in the Round 1 2017 phase of the Australian government smart city plan.

Table 2.5 Smart City Projects in Australia

Project Title	State
• Smart precinct Woden	Australian Capital Territory
• Launceston city 3D modelling	Tasmania
• Switching on Darwin • Smart way to reduce waste	Northern Territory
• Heywood Park smart city precinct • Connected cities prospect • Smart community services excess in mid Murray region • Smart tourism town Kapunda • Smart active transport in Port Adelaide • Connecting communities in Alexandrina	South Australia
• Minimising impacts of urbanisation on the Great Barrier Reef • Automated traffic management, Fraser Coast • Interactive development platform, Ipswich • Sustainable urban growth, Bells Creek • Yeppoon town centre smart precinct project • Digital permits for disability parking, Rockhampton • Streamlined access to community services, Moreton Bay • Smart parking, North Lakes	Queensland
• Resilient energy and water systems, Fremantle • Smart cities collaboration, Perth • Smart monitoring and management, Yellagonga Wetlands • Smart emergency and fire management, Collie • RailSmart planning, Wanneroo • Automated vehicle trial, Perth • Solar energy solutions, Broome • Energy efficient housing, South Perth	Western Australia
• Smart move Newcastle: intelligent mobility, energy and data networks • Smart transport, Macquarie Park • Smart regional city, Queanbeyan • Liveable neighbourhoods in Lake Macquarie and Sydney city • Energy data for smart decision making • Smart transport, Randwick • Smart mobility, Sydney • Smart community infrastructure, Sydney • Community WI-FI and open data, Bathurst	New South Wales

• Smart strategic planning, Byron • Smart active transport, Liverpool • 3D technology for urban planning in Woollahra • Smart parking, Central Coast • Goldenfields water app • Community participation in smart urban planning for Logan and Canada Bay	
• Latrobe Valley sensor network • Clever and creative Geelong • Interactive city management in Melbourne • 3D city planning of Moreland Council • Smart planning and design, Melbourne • Smart planning, Werribee • Smart community services for the Southern Grampians • Smart active transport - urban heat maps for Bendigo • Smart transport and precinct planning, Atherstone	Victoria

The Australian Government smart city and suburb plan indicates a number of projects that are under way and have been identified as smart city projects. A survey by KPMG Australia shows that 80% of the respondents believe the journey of smart cities in Australia has begun with 39% working towards strategic plans development, 15% preparing a detailed roadmap and, most importantly, 26% of Australian councils are now running pilot programs and deploying new projects into their communities (KPMG, 2017). This indicates Australia's move towards smart cities development, and it is the ideal time to evaluate security and privacy concerns in smart cities initiatives that may impact current and future adoption of smart city related services.

The Australian Government's smart cities and suburbs program guideline defines four priority areas for upcoming smart cities projects, which are smart infrastructure, smart precincts, smart services and communities and smart planning and design (Australian Government, 2018). All these smart city projects involve information technology services

such as Internet of Things as facilitating technologies. The smart cities and suburb program aims to improve liveability, productivity and sustainability of the cities, suburbs and towns by applying innovative technology-based solutions to the city and community challenges (Australian Government, 2017). The Australian Government's priority areas are also supported by other studies (Dubbeldeman & Ward, 2015; Hayat, 2016) where authors focus on sustainability, liveability and productivity as key focus areas of the smart cities. Table 2.6 represents the Australian Government's smart city priority areas and their description.

Table 2.6 Australian Smart City Priority Areas

Smart City Area	**Description**
Smart infrastructure	Projects that improve infrastructure related services such as communication, mobility, accessibility, landscape and green infrastructure, emergency response, water supply and waste management.
Smart precincts	Projects that promote better management of public facilities, assets and spaces while improving comfort, amenity and security by the use of integrated and intelligent systems that provide automated responses to real-time environmental and usages data.
Smart services and communities	Solutions to improve public engagement, involve community in service design and delivery, facilitate customers towards decision making by providing access to information, enhance access to council services and help towards availability of real time council data.
Smart planning and design	The smart solutions that provide sophisticated information for better decision making and governance at all levels through automation in data integration from sensors, planning of systems that predict development impacts and smart data analysis tools that analyse data from myriad sources for improvement of land use and planning.

Kickbusch and Gleicher (2014) state that cities and the countryside can benefit from smart city services that actively engage citizens in smarter, participatory governance of their regions. City governments worldwide develop their policies for economic development with

the aim of building advanced infrastructure and implementing smart city initiatives, and this has become a priority on the list of municipal goals.

In summary, this section has provided an overview of real-world smart city projects and their relevance to Australia. The Australian Government plan indicates extensive use of data driven solutions for current and future smart cities. It is reasonable to accept that in a system that involves significant information technology devices and data generation, analysis and sharing, security risks must not be neglected. In fact, the public and open system poses an even greater risk of misuse of such a system for unsolicited activities in smart cities infrastructure. The upcoming section discusses the security and privacy challenges faced by smart cities.

2.7 Security and Privacy Related Challenges in Smart Cities

Advancement in technology is influencing almost every aspect of life as citizens are increasingly dependent on it to perform their daily tasks. The publicly accessible advanced technologies are attainable at reduced cost and are the means of high-speed communication. While technological advances are making everyday tasks easier, faster and more secure, some individuals are interested in illegitimate use of such technologies and deliberately misuse it for different reasons. The unsolicited use of information and technology, whether it be a data breach or denial of service (DoS) attack, are cybercrimes liable to legal action. Bernik (2014) defines cybercrime as a crime assisted by a computer system. The motives for such criminality appear to differ from person to person. However, it is widely agreed that financial gain is the major aim of most cybercrimes unless it is identified as cyber warfare or cyber terrorism, where the motives are broader (Bernik, 2014). Smart cities are facilitated by numerous IoT devices and sensors and IoTs are known for having security vulnerabilities.

Traditional technologies may have similar vulnerabilities, but the scale of cyber security risk increases with the rise in number of IoT devices in use. Various aspects of cyber security and the challenges related to smart city and its technologies will be discussed next.

As the economic benefits from smart cities are seen to grow, there is an increasing need to ensure the systems are digitally secure. For instance, a hacked email account may only have impact upon an individual, but a hacked smart grid system can paralyse a whole city or even a country (Mo et al., 2012). Bartoli et al. (2011) indicate the following security related challenges that should be considered when designing smart city projects.

Privacy: The mechanism for integration of privacy and security is one of the key concerns to consider while planning smart cities projects. A design which cannot ensure privacy for users will be unable to succeed in the market. Privacy breach and information inference by attackers and intruders are major vulnerabilities because sensitive information is generated, transmitted and processed in the smart city infrastructure (Zhang et al., 2017).

Network Connectivity: An unsecure network opens the door for multiple threats via various cyberattacks. While keeping networks private and isolated minimises threats, smart cities require a widely interconnected network grid which opens the door to multiple cyber threats.

Complexity: The complexity of the network of devices and systems needs to be minimised to facilitate an accessible and manageable system. Complex architecture is usually uncooperative towards security and diagnosis.

Security Services: Smart cities require access to high quality, cost effective security services including expertise in the different fields such as mobility, security and system integration.

Sensitive Data Organisation: With the implementation of a smart city plan, the users and their sensitive data will increase and organising such a high volume of sensitive data requires adequate skills and expertise. State-of-the-art provisions are required to manage private and sensitive user data generated by IoT devices in smart cities.

Buntz (2017) supports the notion that cyber security is a widespread concern for a majority of smart city projects. A survey conducted by Dimensional Research found that more than half of information technology professionals from a survey of 203 participants believed that the cities they lived in were not adequately concerned about cyber security. The Dimensional Research's survey reported that 27% of respondents believed the public wireless networks were at major risk, 18.6% thought smart grids are at more risk while 12.7% said public lighting was the most vulnerable system in a smart city (Buntz, 2017).

Similarly, Commissioner for Privacy and Data Protection, CPDP (2018) indicates some of the key security and privacy issues of the smart cities include data handling, privacy in sharing of information, security risk management, malicious attacks, human error, chilling effect (potential behavioural change of people because of surveillance on them) and the governance issues of the smart cities entities (questions around ownership of technology, data and management of smart cities). Smart cities challenges are still under study as every author describes the challenges based on their own perception. The security challenges indicated above are overall cyber security challenges of the smart cities. The devices and technologies

used in Australian smart cities may present unique challenges related to regional variations in factors such as population, economy, infrastructure and more.

2.7.1 Factors Influencing Security in Smart Cities

A number of security related factors make smart city services and technologies vulnerable to attackers and intruders. Baig et al. (2017) conducted an exploratory literature survey, along with case studies, to compile the security landscape of smart cities, mainly focused on Smart Grids, Building Automation Systems (BAS), Unmanned Aerial Vehicles (UAVs) sensors and cloud computing horizon. The main security threats indicated by Baig et al. (2017) are summarised in Table 2.7.

Similarly, Elmaghraby and Losavio (2014) suggest that unauthorised interception of real-time transportation data may create unexpected risk towards personal safety because of location services data vulnerability. The authors also agree that privacy is the major concern in smart transportation because of possible location data vulnerabilities associated with it. Hasbini and Martin (2017) point out the challenges related to traditional access control methods in IoT device network and provided the modified version of the access control method for IoT devices. Since smart cities possess millions of interconnected IoT devices, access control is deemed to be one of the major security issues requiring effective solution. Similarly, Cilliers and Flowerday (2015) investigated crowdsourcing systems in the smart city to identify the relationship between privacy, information security and the perceived trustworthiness to increase citizens' participation in the system. The study finds a positive relationship between privacy and perceived trustworthiness of the crowdsourcing system. The authors suggested adequate information security controls can enhance trustworthiness of the crowdsourcing system in the smart city. This promotes an affirmative relationship between privacy and trust

factors towards the user's participation in new technology. However, this study fails to identify what specific security measures can earn trustworthiness of city inhabitants or users.

Table 2.7 Security Threats of Smart City Related Services

Smart City Dimensions	Associated Security Threats
Smart Grids	• Protocol vulnerabilities • Privacy • Eavesdropping • Rogue or infected devices • Attacks on devices connected to internet
Building Automation System (BAS)	• Highly trusted devices • Long lifecycle of devices • Authentication issues • Vulnerable protocols
Unmanned Aerial Vehicles (UAVs)	• Intercepted communication • Malicious Code injection • Communication jamming
Smart Vehicles	• Physical threats • Communication interception • Communication jamming or denial of service attack • Data security
IoT Sensors	• Maintaining data confidentiality • Secure communication • Data management and storage • Sensor failure • Remote exploitation
Cloud	• Data leakage • Malicious insider's threat • Insecure Application Programming Interfaces (APIs) • Denial of service attacks (DoS attack) • Malware injection attacks • System and application vulnerabilities • Data location and data regulation boundaries

Source: Baig et al. (2017)

Further emphasis is given on smart city's security by Ijaz et al. (2016), who claim that to guarantee the continuity of critical smart city services, cyber security needs to be robust. The authors here tried to identify security issues in smart cities by looking at governance, socio-economic and economic perspectives. They identified various security issues categorised into those three perspectives. The technological perspective mostly involves IoT devices, semantic web, cloud computing, databases, software and artificial intelligence. Similarly, the governance perspective involves utility, health, education, infrastructure, transport, energy and environment whereas the socio-economic perspective includes communication, privacy, business finance, and commerce. This indicates there is not a single factor responsible for information security and privacy in smart city infrastructure. The authors also provided the possible solutions for smart cities' IoT vulnerabilities but argue that the excellent functionality of these devices has no value if the system has security issues. They believe that manufacturers and decision-making authorities are responsible for ensuring the security of these IoT devices and systems. Figure 2.5 shows the relationship among factors influencing information security (Ijaz et al., 2016).

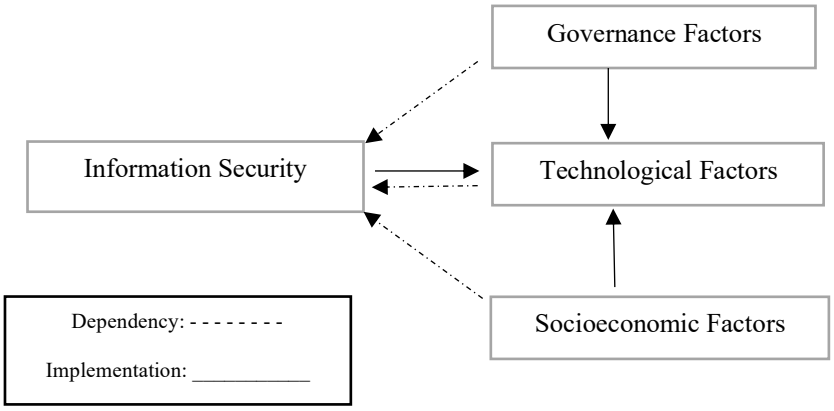


Figure 2.5 Relationships Between Factors Influencing Information Security

Source: Ijaz et al. (2016)

2.7.2 Security Risks Related to IoT and Big Data in Smart Cities

Zhang et al. (2017) represent the risk of insiders in smart city organisations towards cyber security because most of the existing smart city architecture and security solutions are focused on defending risk from outside attackers and intruders. Insider risks are believed to stem from any employees who have easy access to systems and data. The authors also emphasise the risk to smart city security and privacy including privacy leakage in data sensing, privacy in data storage and processing, and trustworthy and dependable control. The literature above fairly supports IoT as a backbone of the smart city services. Therefore, it is essential to explore the security aspects in IoT dimensions as well. The following section provides an overview of the security aspect of IoT in smart city.

Data is at the centre of every organisation regardless of type. Smart cities generate huge amounts of data by their underlying IoT sensors. Some data will be designated as higher security than others.It is a well agreed fact that one of the major security challenges of smart cities is data security and privacy. Gharaibeh et al. (2017) conducted research to provide a holistic approach to manage smart city data with security and privacy as major considerations. Some technologies that generate data in smart city environments are sensor networks for smart streetlights, smart traffic management, virtual power plants, smart emergency systems and smart health, mobile ad-hoc networks, virtual ad-hoc networks, IoT devices, unmanned aerial vehicles, social networks and crowdsourcing (Gharaibeh et al., 2017). However, the data generating smart city technologies are not limited to certain sensors or systems but may also include a wide range of technology and services being implemented throughout the city.

Elmaghraby and Losavio (2014) discuss the various activity nodes that generate information in the smart cities via many interconnected instruments, as personal life, social life, work life, transport and home life. The authors claim that security and privacy concerns of those smart cities' information rest on how information is used within three major components of smart cities: instrumented, interconnected and intelligent. Figure 2.6 shows different locations where the smart city data are generated in everyday life.

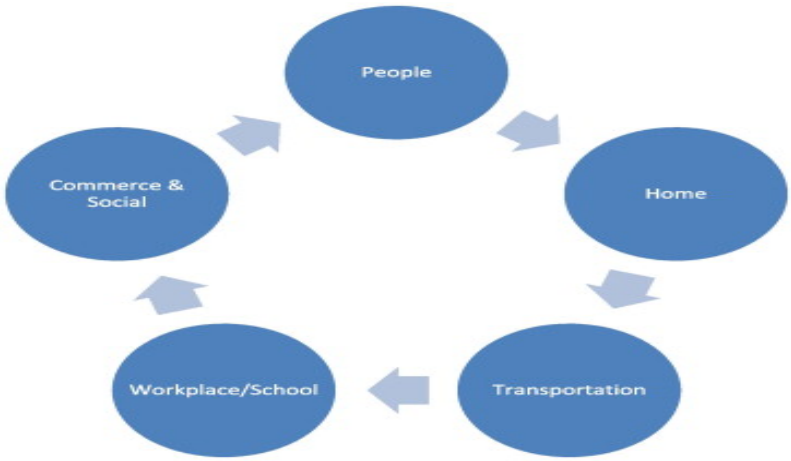


Figure 2.6 Locations of Data Produced in Smart City

Source: Elmaghraby and Losavio (2014)

The enormous amount of data generated in smart cities requires big data solutions to gain insight from the data and make data driven decisions. Bibri (2018) emphasises the application of ICT towards smart cities with big data solutions. It is accepted that large-scale real-time data is generated by numerous IoT sensors and devices in smart cities. The real time generation of a large volume of data also requires real-time storage, processing, query and analysis of big data (Deren et al., 2015). However, big data applications for smart cities bring many challenges. Al Nuaimi et al. (2015) claim security and privacy as one of the major challenges of big data application to smart cities while other challenges outlined relate

to data sources and characteristics, sharing of data and information, quality of data, cost, and population of the smart cities. The privacy and security issues for a smart city's big data application are mainly related to risk to government and citizens' confidential data from malicious attacks. More importantly, big data technologies such as Cassandra and Hadoop are labelled as having insufficient security (Kim et al., 2014). The security and privacy issues are likely to influence the adoption of a smart city's big data applications.

IoT, being the backbone of the smart cities, can support a number of applications and services that benefit society in personal and economic ways. Several definitions exist to conceptualise IoT as it is an emerging field of interest that consists of a number of technologies. The main purpose of IoT is to allow users to distinctly identify, signify, access, and control devices via the internet from any location at any time (King & Awad, 2016). Granzer et al. (2006) believe that one of the applications of IoT is smart homes, as the concept of smart homes focuses on automation and control of home environmental control services like lighting, central heating, ventilation and air conditioning. Similarly, Al-Qutayri and Jeedella (2010) claim that the focus of the IoT integration in smart homes is on monitoring and control, safety, security and energy savings. A recent study conducted by Ali and Awad (2018) assessed cyber security vulnerability of smart homes and found that the human factor is the key player towards security risks. Their study regarded IoT as a main enabling technology for smart homes. The authors also identified that people with less technical knowledge are prone to social engineering attacks and also tend to misuse systems.

Jing et al. (2014) compared the security issues between traditional network and IoT network and concluded that IoT networks were highly vulnerable in comparison. Similarly, Chakrabarty and Engels (2016) propose basic components of the secure IoT framework for

the smart city. The authors represent black networks, trusted software defined networking (SDN) controller, unified registry and key management as the security solution for IoT architecture.

Various literature indicates there are three important characteristics of the information security: confidentiality, integrity and availability (Chen, 2017; Huntley, 2010; Zissis & Lekkas, 2012). Compromising any of these three security characteristics leads to security damage of the IoT system (Chen, 2017). Firstly, confidentiality in the IoT system means data collected from the various IoT devices should not be exposed or transmitted to an unauthorised party. There are various mechanisms available for ensuring confidentiality such as encryption, multi-factor authentication, and public key infrastructure. Secondly, integrity is the mechanism to ensure information is not changed during communication or while in storage servers. Lastly, availability ensures data and services are available at any time without loss or distraction. Figure 2.7 presents the confidentiality-integrity-availability (CIA) triad of the information security related to IoT. Some of the well-known IoT security issues are Denial-of-Service (DoS), distributed denial of service, middle attacks and heterogeneous network attacks (Jing et al., 2014).

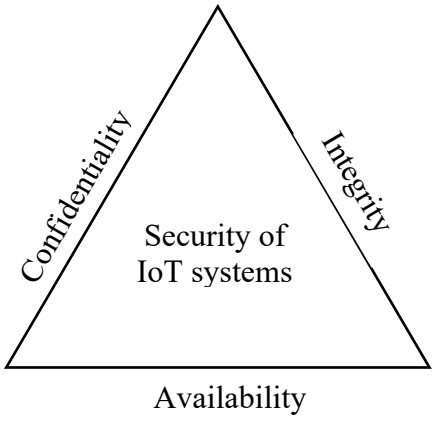


Figure 2.7 IoT Information Security Triad

Source: Chen (2017)

One of the widely used methods to identify and assess existing security risk in any information technology infrastructure is security risk assessment. The most popular and well-known risk assessment tools include NIST SP800-30, ISO/IEC 27001, OCTAVE, CRAMM and EBIOS which all originate from the standardising bodies such as NIST and ISO/IEC or government bodies such as CRAMM and EBIOS (Nurse et al., 2017). Despite having multiple risk assessment methods, Nurse et al. (2017) also argue that existing security risk assessments have limitations, so are not useful for assessing information security risk of IoT devices and infrastructure. This fact indicates the unsuitability of current risk assessment frameworks for identification of security risk in IoT infrastructure such as smart cities.

To sum up, IoT is an integral part of the smart city infrastructure, and smart city's security challenges are closely related to the challenges of IoT technology used in smart city infrastructure. IoT security, along with communication channel and security of data involved, are integral parts of smart city security. Further, Smart city stakeholders' perception on information security aspects related to smart city and their intention to adopt smart city services, are the key to determine factors influencing the success of smart city initiatives. The various sources of literature reviewed suggest smart city services are valuable for solving urban problems with the help of technology and to increase liveability, sustainability and productivity. This is the stated objective of the Australian Government's smart cities and suburb programs. However, the literature presents limited evidence on smart cities adoption in Australian cities, let alone the effect of security and privacy on trust in the smart city services adoption by regional Australian cities. A report by the Australian Government (2018), indicates many regional cities are suffering from low or negative growth, as jobs lost in the manufacturing sector, or more recently the resources and energy sectors, are not replaced quickly enough. It is therefore critical for the government to plan for regional cities

to reach their full potential through maximising their unique advantages and supporting their long-term growth through the development and implementation of smart city services. Therefore, this study provides a comprehensive review of factors that influence stakeholder's trust towards their intention to adopt smart city services in Australian regional cities. This study aims to understand the role of security related factors in influencing stakeholders' trust towards their intention to adopt smart city services.

2.8 Conclusion

This chapter provided an overview of smart cities, their dimensions and their role along with security related issues. Smart city is a broad concept with several dimensions and several underlying technologies and services working together. The security issues are not concerned with a single technology but have a broad reach as different smart city related technologies have different problems and risks associated with them. So, this chapter has provided an important foundation to understand smart city, associated technologies and security concerns. The review of literature shows that there are a number of widely accepted smart city initiative frameworks. Proposed frameworks have mostly utilised the dimensions that are used in the study of e-government and other commercial e-services acceptance by respective users. Smart cities have various dimensions and entities that represent related services. As suggested by the literature review, security and privacy related concerns are foremost regarding development and adoption of innovative and new technologies, which are also related to smart cities. Further, there are limited studies available that explore the influence of security related determinants towards trust and adoption of smart city services by stakeholders. This research expects to provide valuable knowledge towards determining the influence of factors related to technological, organisational, environment and security

dimensions. Chapter 3 provides the conceptual framework for the research by exploring various studies related to smart city adoption.

3 Conceptual Framework

3.1 Introduction

This chapter reviews the literature in relation to technology adoption models and develops a conceptual framework for the study of trust-based smart city adoption. Section 3.2 provides background information about the context of the research domain. Section 3.3 reviews some of the models used in the technology adoption studies. Trust factors in the context of technology adoption studies are the subject of Section 3.3.3. Further, Section 3.4 discusses each factor used in the theoretical framework as supported by prior studies. Finally, Section 3.5 concludes the chapter. The organisation of this chapter is presented in Figure 3.1.

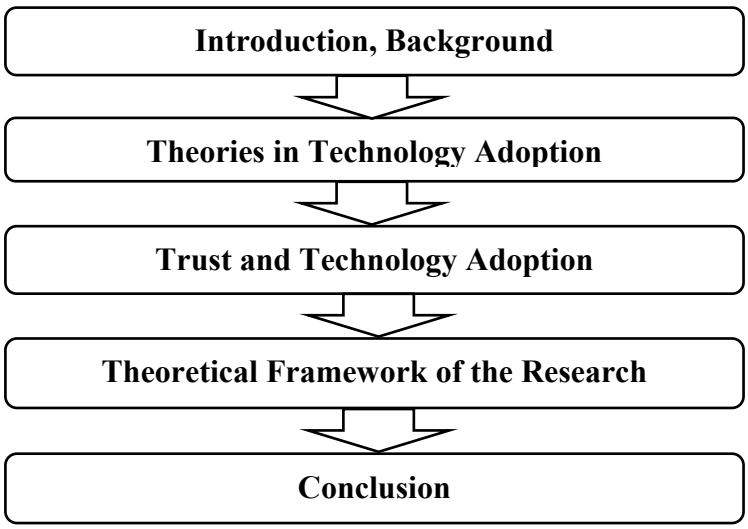


Figure 3.1 Overview of Chapter 3

3.2 Background

The term ‘smart city’ is increasingly used in academia, and scholars are exploring various dimensions of smart cities and related technologies (Letaifa, 2015). The services and solution capabilities of smart city services can motivate the industry towards incorporation of information technology led smart solutions. ICTs are claimed to be at the core of smart cities, which focus on enhancing socio-economic, ecological, logistic and competitive functioning of the cities (Kourtit & Nijkamp, 2012). These enhancements of city operations by the use of ICTs make smart city services popular. There is no doubt that smart cities are enabled by numerous interconnected Internet of Things (IoT) devices, cloud computing and artificial intelligence.

Despite the benefits, there are security and privacy related challenges that often influence the adoption of ICT related services. Almuraqab and Jasimuddin (2017) point out security related challenges as key influencing factors towards the adoption of smart cities. This is further supported by Braun et al. (2018) and Dewi et al. (2018), where they claim that security and privacy are major concerns for adopting smart city related services. The use of innovative and smart technologies for smart city transformation is essential, but the intention to adopt the available technologies by its stakeholders is more important for its success. Trust plays a vital role towards acceptance of innovative technology as it is widely used in the technology adoption studies (AlHogail & AlShahrani, 2018; Bose et al., 2013; Ratten, 2014; Yeh, 2017). According to Mayer et al. (1995), trust is the readiness to be vulnerable by the actions of another party. It is identified as a critical component for technology adoption, because it addresses risk vulnerability and uncertainty (Pavlou et al., 2003). Trust and security are inter-related in adopting new technologies as individual’s belief on security may have an influence on their intentions. In fact, previous studies considered trust as a factor in predicting intention

behaviour (Belanche et al., 2012). Although, previous studies conducted by Chourabi (2012), Dewi et al. (2016) and Van Zoonen (2019) focused on the importance of security and privacy for the adoption of smart cities through the development of a security model, these studies were limited to technology, organisation and environmental factors and did not considersecurity and privacy.. The study of smart cities is still in its infancy, so the smart city services and security and privacy are theorised based on similar information technology services and security. Security in the information and technology domain is broadly defined within the dimension of confidentiality, integrity and availability (Chen, 2017; Zissis & Lekkas, 2012). To support this Huntley (2010) also emphasises that confidentiality, integrity and availability are necessary attributes to be considered to ensure data and device security in a real-time world. The proposed research assumes that security of the smart city services should fulfil the abovementioned three characteristics of information security. However, the following section will expand on the concept of information security and how different variables related to information security may influence adoption of smart city services.

The conceptual framework here also includes several important variables from the information security compliance model used by AlKalbani et al. (2015). The authors have adopted the Technology-Organisation-Environment (TOE) and institutional theory to develop their information security compliance model. The compliance of information security represents the reliability of the technologies used in the organisations that satisfy the policies and standards related to information security and improve compliance by enhancing users' trust and confidence in using the technology (AlKalbani et al., 2015).

3.3 Theories Used in Technology Adoption

It is noteworthy that acceptance and adoption with confidence are crucial towards the success and further development of innovative technologies. Decision makers should know the issues that may impact a users' decision to use a system so that they can consider such issues during the development phase of such systems (Mathieson, 1991). Acceptance of a technology has been regarded as a result of users' involvement in the system development (Taherdoost, 2018). This means it is important to look at the theories used in acceptance and adoption of innovative and new technologies. Further, it is suggested that multiple theoretical approaches are necessary to have a complete picture of the concerns involved, and for precision, different approaches are looked at independently (Taherdoost, 2018). The most established theories in adoption and acceptance of technology are Diffusion of Innovation (DOI) (Rogers, 1995), Technology Acceptance Model (TAM) (Davis, 1989), Unified Theory of Acceptance and Use of Technology (UTAUT) (Venkatesh et al., 2003), Human Organisation and Technology (HOT-fit) (Yusof et al., 2006) and Technology-Organisation-Environment (TOE) (Tornatzky & Fleischer, 1990). The established models such as TAM, UTAUT, HOT and TOE are widely used for the innovation adoption studies. The following sections will briefly discuss some of the research models used in the study of technology adoption, but more emphasis is given to the use of TOE model in the adoption of smart city services and innovative technologies.

3.3.1 Technology Acceptance Model (TAM)

TAM is a widely accepted and used framework that theorises user acceptance and use of technology and technology related services (Davis, 1989). TAM proposes that actual use intention of the technology is derived by the perceived ease of use and perceived usefulness of that technology. TAM originally adapted the theory of reasoned action (TRA), which is a

very popular model of social psychology that mainly focuses on the determinants of consciously intended behaviour (Chuttur, 2009). TAM represents intention to adopt technology influenced by various external factors. Trust variables in this study are designed to be influenced by four categories of external factors, which are technology, organisation, environment and security. AlHogail (2018) uses product, social influence and security as factors determining trust and intention to adopt IoT technology, where the author has used TAM as the base model for theoretical framework used in the study. Figure 3.2 presents TAM by Davis (1989).

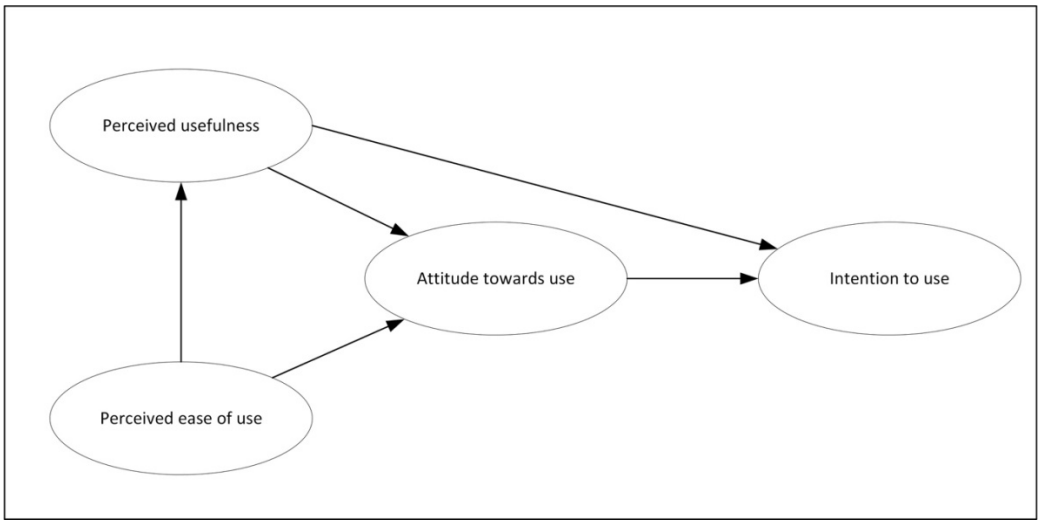


Figure 3.2 Technology Acceptance Model (TAM)

Source: Davis, (1989)

A number of studies such as (Park et al. (2017), Toft et al. (2014)) have introduced new variables into the original TAM model to fit the study context. Table 3.1 shows the list of studies that adopted TAM and its variations for the technology adoption studies.

Table 3.1 TAM based technology adoption studies

Model used	Study context	Variables used	Reference
TAM	User acceptance of internet of things in a smart home environment	Perceived compatibility, perceived enjoyment, perceived connectedness, perceived control Perceived usefulness, perceived ease of use, attitude, perceived cost, intention of use,	Park et al. (2017)
TAM	Adoption of e-government	perceived usefulness, perceived ease of use, trust issues, subjective norms and computer self-efficacy	Dahi and Ezziane (2015)
TAM	Consumer acceptance of smart grid technology	Perceived usefulness, perceived ease of use, personal norm, attitude, acceptance	Toft et al. (2014)
E-service TAM (ETAM)	User acceptance of e-service technology	User friendly, training, performance, trust, design, usability, content, support, interaction, expectation, satisfaction, quality, security, intention to use and acceptance	Taherdoost (2008)
TAM	Original TAM	Perceived usefulness, perceived ease of use, attitude towards use, intention to use	Davis, (1989)

3.3.2 Technology-Organisation-Environment (TOE) Framework

As initially proposed by Tornatzky and Fleischer (1990), the TOE framework involves several attributes categorised into three dimensions -, technology, organisation, and environment. TOE framework has been increasingly popular for studies related to adoption of innovative technologies. The dimensions of TOE framework as presented in Figure 3.3 are listed below:

- Technology factor focuses on how adoption of innovative technology solution is influenced by structure, quality and characteristics of the technology.

- Organisation factor represents the influence of organisational factors such as organisational structure, culture, objective, decision making process, and quality of resources, towards the adoption and acceptance of innovative technologies.
- Environment factor represents how the external attributes of the organisation such as competitors, suppliers, customers, governments, and communities influence towards organisation's ability to determine and facilitate the innovation.

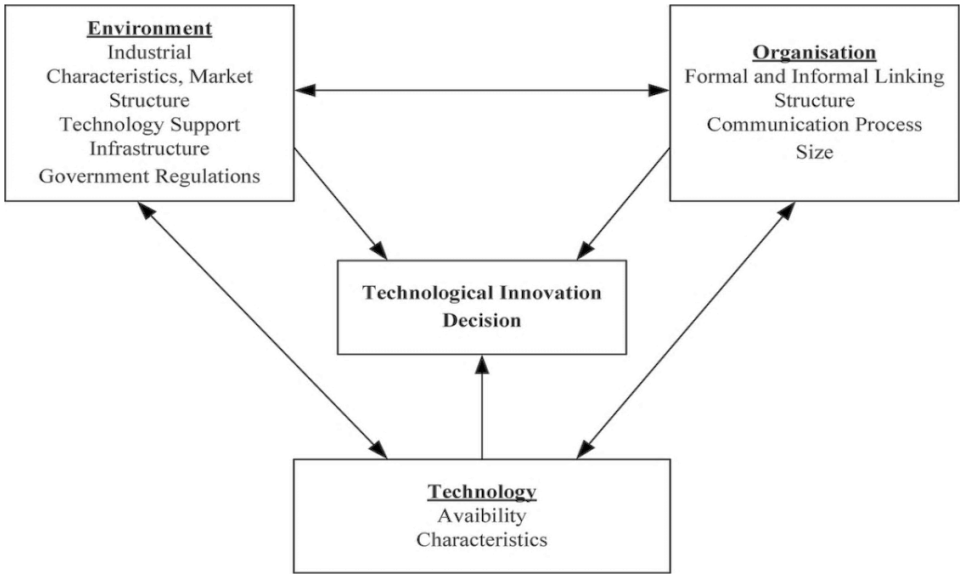


Figure 3.3 Technology Organisation Environment (TOE) Framework

Source: Tornatzky and Fleischer (1990)

Grandhi et al. (2019) develop a security-HOTE-fit framework to identify key security related determinants for intention to adopt cloud computing technologies in Australian councils. The authors combined TOE model and Human-Organisation-Technology (HOT) model to develop a new model that uses variables focused on security aspects as illustrated in Figure 3.4.

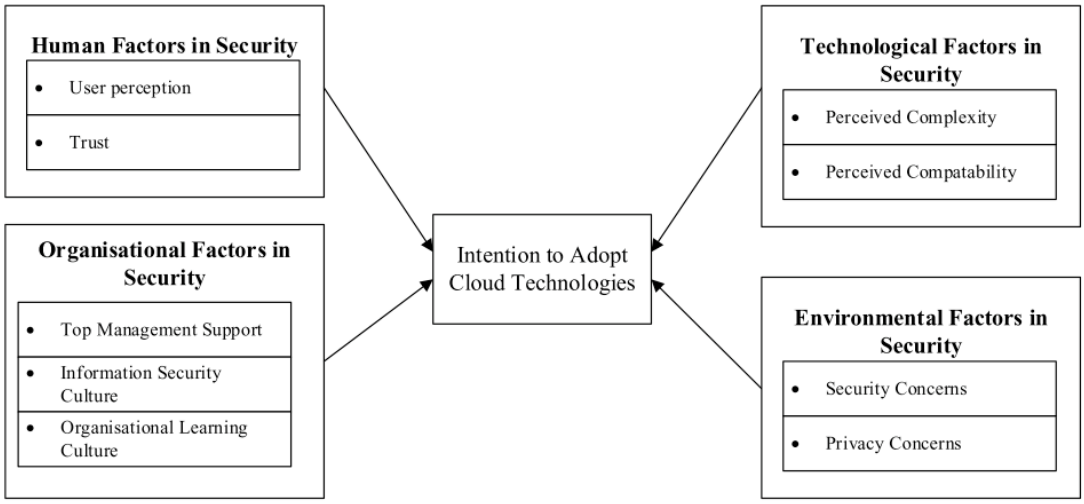


Figure 3.4 Sec-HOTE-Fit Framework

Source: Grandhi et al. (2019)

Table 3.2 lists several studies that apply the TOE framework and derived models in the adoption of technology and related services. TOE framework has been used by many researchers to study adoption of information technology related services such as information security culture (Mokwetli & Zuva, 2018), smart city adoption readiness (Dewi et al., 2018), adoption of big data solutions in organisations (Salleh & Janczewski, 2016), and cloud computing adoption (Yoo & Kim, 2018).

Table 3.2 Studies on Technology Adoption Based on TOE Framework

Model	Study on adoption of technology	Authors
TOE	Adoption of ICT security culture in small, medium and micro enterprises.	Mokwetli and Zuva (2018)
TOE (TOE readiness)	Influence of Technology, organisation and environmental readiness towards smart city adoption decisions by local governments.	Dewi et al. (2018)
TOE and Human Organisation Technology (HOT)	Security determinants on cloud computing adoption by organisations. Study based on survey and interviews.	Grandhi et al. (2019)
Sec-TOE	Adoption of big data solutions by organisations.	Salleh and Janczewski (2016)
TOE	Decision making model for cloud computing adoption.	Yoo and Kim (2018)
TAM and TOE	Determinants of cloud computing adoption.	Gangwar et al. (2015)

AlHogail (2018) propose a technology trust model to study adoption of IOT technologies by consumers. The author categorised variables into three dimensions such as product related, social influence related and security related dimensions. The study concludes security related factors as most significant for determining consumers' trust towards adoption of IoT technologies. Figure 3.5 presents the IoT Technology Trust model proposed by AlHogail (2018).

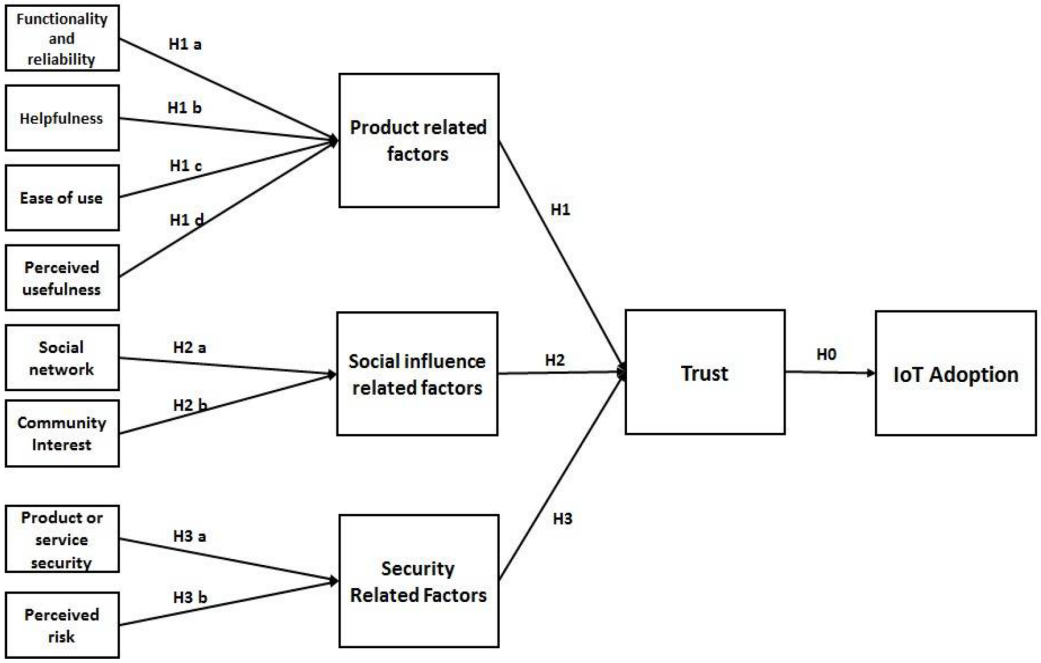


Figure 3.5 IoT Technology Trust Model

Source: AlHogail (2018)

Several scholars have proposed various theories for the adoption of innovative technologies. Of these, most notable are Technology Adoption Model (TAM) (Davis et al., 1989) and Technology, Organisation and Environment (TOE) model. TAM proposes that actual use intention of the technology is derived by the perceived ease of use and perceived usefulness of that technology (Davis, 1989). Meanwhile, TOE model categorises technology adoption related attributes into three dimensions namely, technology, organisation and environment (Tornatzky & Fleischer, 1990). The TOE model has been used widely to study the technology adoption intention, and acceptance of new and innovative technologies. It identifies technology, organisation and environmental factors as influencing factors in technology adoption in organisations (Tornatzky & Fleischer, 1990). The technology factor explains adoption in terms of functionality and reliability as well as their perceived usefulness. The scholars point out that information system culture plays an important role in technology adoption decision. The environmental context refers to pressure from external

partners and government policy. The TOE model considers social and behavioural aspects to determine the interaction among technology development in an organisational setting influenced by the surrounding environment (Hossain & Quaddus, 2011).

As cities and towns are public entities, the TOE model can be useful in assessing the smart city services and technologies adoption intention (AlHogail, 2018; Dewi et al., 2018). This is because this model includes the study of environmental-related factors crucial in the development and implementation of smart city technology (Grandhi et al., 2019). For instance, Dewi et al. (2018) successfully used the TOE model to assess the influencing factors towards smart city adoption decision by public organisations. Gangwar et al. (2015) used the TOE model to study key determinants of cloud computing adoption. While the TOE model offers a valid ground for studying technology adoption intention, it does not consider the security context in technology adoption.

3.3.3 Trust-Based Technology Adoption Models

Trust denotes the willingness of a user to assume the risk of information disclosure (Mayer et al.1995). The representation of trust by Koller (1988) as a function of an extent of risk of a certain situation can be alternatively viewed as a function of a smart service user's risk. This means that when there is minimum risk of security in the smart services, there would be more trust towards such service or system. A number of prior researchers have used and indicated trust as a significant factor towards adoption of technologies. Table 3.3 indicates that a number of existing studies have emphasised that trust plays an important role towards adoption of technologies. However, the variables used in the adoption studies are different depending on the context of the study. The relationships of trust are identified with privacy, policy, usability, organisational culture, intention to use, intention to adopt, security along

with other socio-cultural and human factors as summarised in Table 3.3. For example, Bose et al. (2013) believe that access control and availability, confidentiality and privacy, and long-term viability and regulations are important factors in building trust in technology adoption. On the other hand, Lippert and Swiercz (2005) stated that organisational culture should also be considered in technology adoption. Dahlberg et al. (2003) believed that institutional-based structural assurance and intention to use need to be considered for enhancing trust in technology adoption.

Table 3.3 Technology Adoption Studies That Use Trust Factor

Research Context	Variables	Authors
Role of security and trust in technology adoption. Comparison between banking and cloud computing	Critical security thinking, access control and availability, confidentiality and privacy, and long-term viability and regulation	Bose et al. (2013)
Influence of technology trust towards successful implementation of human resource information system	Technology adoption, technology utility, technology usability, organisational trust, pooled interdependence, organisational community, organisational culture, socialisation, sensitivity to privacy, predisposition to trust	Lippert and Swiercz (2005)
A trust enhanced adoption model for mobile payment solutions	Calculative based, institutional based structural assurance, institutional based situational normality, knowledge-based normality, perceived ease of use, trust, perceived usefulness, intended use	Dahlberg et al. (2003)
Role of trust, innovation and performance in behavioural intention to adopt technological innovations	Innovation attitude, social norm, performance expectation, trust and intention to adopt as independent variable	Ratten (2014)
Improving IoT adoption by improving consumer trust	Intention to adopt is determined by trust and trust influenced by product, social influence and security related factors	AlHogail (2018)
Determinants of acceptance of ICT based smart city services and its effect towards quality of life	Trust dependent on perceived privacy Acceptance of ICT based smart city services determined by personal innovativeness, innovation concept, city engagement, service quality and trust. Acceptance of ICT based smart city services determine quality of life	Yeh (2017)

The analysis of various technology adoption models and importance of trust factors in smart city related technology adoption has concluded that factors within the dimensions of technology, organisation, environment and security can be used to assess their influence towards trust before assessing influence of trust towards adoption intention. TOE model has been previously used in a study related to smart city adoption (Dewi et al. 2018). Further, other studies conducted for adoption of smart city's enabling technologies such as cloud computing and IoTs used TOE model. Thus, selection of TOE model for the current study is supported by the prior studies that use this model for the adoption of smart city and its related technologies. A number of studies summarised in Table 3.3 show trust variable is used for the study of technology adoption. The relationships of trust are identified with privacy, policy, usability, organisational culture, intention to use, intention to adopt, security along with other socio-cultural and human factors as summarised in Table 3.3. For example, Bose et al. (2013) believe that access control and availability, confidentiality and privacy, and long-term viability and regulations are important factors in building trust in technology adoption. On the other hand, Lippert and Swiercz (2005) stated that organisational culture should also be considered in technology adoption. Dahlberg et al. (2003) believed that institutional based structural assurance and intention to use need to be taken into account for enhancing trust in technology adoption. There is positive influence found between trust and adoption intention (Ratten, 2014) and trust is influenced by several technological, organisational and security factors as summarised in Table 3.3. Therefore, combining TOE and security related variables with trust is formulated as a suitable theoretical approach for assessing trust-based adoption intention of smart city services and technologies. The next section will discuss the theoretical framework of the research.

3.4 Theoretical Framework of the Research

The theoretical framework developed in this study is based on the TOE model. The TOE model presents a number of dimensions that have an influence towards adoption of technologies in organisations (Tornatzky & Fleischer, 1990). Scholars have widely used the TOE model to study the technology adoption intention, and acceptance of innovative technologies. For instance, Dewi et al. (2018) apply the TOE model to assess the influencing factors towards smart city adoption by public organisations. Meanwhile, Gangwar et al. (2015) use the TOE model to study key determinants of cloud computing adoption. Considering cities and towns as public entities, the TOE model can also be useful to assess determining factors towards trust and intention to adopt smart city services. As this study aims to study the security related factors that influence stakeholders' trust towards their intention in adopting smart city services, the developed framework adopts information security related factors categorised into various dimensions. Table 3.4 presents the variables used in the research framework, their definitions and the related studies.

Table 3.4 Variables Used in the Study and Their Definitions

Factors	Definition	References
Functionality and reliability	It refers to capacity and ability of specific technology to provide the required features and functions for a specific task ensuring consistent and proper operations as predicted	AlHogail (2018); McKnight et al. (2011)
Perceived usefulness	The extent of user's belief that use of technology would enrich their job performance	Almuraqab and Jasimuddin (2017); Davis (1989); McKnight et al. (2011);
Information security culture	Information security culture is a subdomain of the organisation culture where it supports information security to become imminent part in employee's daily activities	Almuraqab and Jasimuddin (2017); Grandhi et al. (2019); Hameed and Arachchilge (2016)
Pressure from external partners	It refers to the pressure from other businesses such as partners or stakeholders in the supply chain that affects information security	Hashim et al. (2015); Ma and Ratnasingam (2008)
Government policy	Government standards and regulations that may influence a business in terms of information security implementation	Lian et al. (2014); Ma and Ratnasingam (2008)
Self-efficacy in information security	One's belief in capability to safeguard the information and system from unauthorised disclosure, manipulation, loss, destruction, and non-availability	Dewi et al. (2018); Rhee et al. (2009)
Perceived privacy	The tendency to be concerned regarding submitted personal information to the services including safety of possible monitory transaction with services	Dewi et al. (2018); Rauniar et al. (2013); Van Zoonen (2016)
Perceived security	The probability by which users or consumers believe that their sensitive information will not be tampered with by either viewing stored data or manipulated during transmission or storage by unauthorised persons	Chellappa and Pavlou (2002); Dewi et al. (2018); Hameed et al. (2012)
Trust	Probability that a participant in a transaction will act in beneficial way or at least not harmful way to other participants so that they can cooperate later	AlHogail (2018); Almuraqab and Jasimuddin (2017)

3.4.1 Technology Related Factors

Technology can provide the required features and functions to perform a specific task (AlHogail, 2018), but trusting a technology significantly depends on its ability to perform a task (Lian et al. 2014). The following sections discuss the factors that have been identified as

related to technology that influence stakeholder trust towards their intention to adopt smart city services.

3.4.1.1 Functionality and Reliability

Functionality and reliability refer to whether a technology can provide the required features and functions to perform a specific task or fulfil a task requirement as expected (AlHogail, 2018). Trusting a technology significantly depends on its ability to perform a task and has a positive influence towards trust as well as adoption of smart city technologies such as IoT (Lai et al., 2011). Similarly, McKnight et al. (2011) propose trust as a function of functionality, reliability and helpfulness and the authors found the proposed positive relationship between them as significant. This means individuals' trusting beliefs are influenced by functionality and reliability of the specific technology. Based on these prior outcomes, functionality and reliability has been proposed as one of the technology related factors and hypothesised as:

H1: Functionality and reliability has positive influence towards stakeholders' trust in smart city services.

3.4.1.2 Perceived Usefulness

Perceived usefulness as defined by Guriting and Oly Ndubisi (2006), is the subjective probability of users' completion of a given task in an improved way. Mou et al. (2017) examine how trust interacts with consumer beliefs such as perceived usefulness in regard to the consumer's intention to accept the e-services and found a positive relationship between them. The authors also believe that the study of perceived usefulness and trust can have implications towards understanding the dynamic nature of trust and perceived usefulness during different phases of a user's encounters with e-services. Colesca (2009) also found in a

study that perceived usefulness enhances the trust level in e-government services. Direct positive impact of perceived usefulness towards perceived trust has been found by Roca et al. (2009) in a study to examine influence of TAM constructs along with perceived trust towards their intention to adopt an online trading system. Similarly, in a study by Jaafreh (2018), the author found positive influence of perceived usefulness towards adoption of IoT in small and medium enterprises. As supported by various past studies, perceived usefulness is an important determinant towards trust and intention to adopt technology related services. The following hypothesis is proposed for perceived usefulness:

H2: Perceived usefulness of the smart city services positively influences stakeholders' intention to adopt smart city services.

3.4.2 Organisation Related Factors

The organisational context of the framework refers to the multiple characteristics that represent an organisation in general in terms of its strategies, culture, structure and policies (Teo et al., 2006). The organisation domain of the conceptual framework developed for this study involves only one factor, which is information security culture.

3.4.2.1 Information Security Culture

Achieving a secure environment for information is assumed to be an essential part of the organisational culture because information security has become an inevitable part of the business process of an organisation. Information security culture is a subdomain of the organisation culture where it supports information security to become an imminent part in employees' daily activities (Schlienger & Teufel, 2003). Information security culture is also linked to the belief of individual employees towards compliance with organisational policies and standards related to information security (McIlwraith, 2006). There are not sufficient

studies that test the relationship between information security culture and stakeholders' intention to adopt smart city services, so the best way to justify the relationship would be by looking through the organisational perspective. Literature related to e-government information security can also be used to develop a theoretical background related to smart city security culture as literature of e-government have been used to develop a popular smart city integrative initiative model by Chourabi et al. (2012). The security culture of employees in an organisation is created by instilling the concept of information security in every employee as usual duty of performance in the workplace. A higher level of information security compliance as a result of having effective information security culture has been found by AlKalbani et al. (2015), where the research was conducted in the context of e-government services. It is reasonable to relate information security culture and adoption of smart city services by its stakeholders.

One of the key information security risks in organisations results from human behaviour (Workman et al., 2008). According to Alnatheer and Nelson (2009), employees' understanding of appropriate information security culture results from effective training and awareness programs. In an organisational context, information security awareness is an employee's knowledge and understanding about the information security policy and procedures of the organisation, but in general, information security depicts an employee's overall understanding and knowledge about the information security issues and their ramifications (Bulgurcu et al., 2010). Information security culture and awareness has also been indicated by Conklin and White (2006) as an important influencing factor for adoption of the e-government system by its users. Therefore, the following hypothesis has been proposed relating information security culture and stakeholders' trust in smart city services and technologies.

H3: Stakeholders' security culture positively influences stakeholders' trust in smart city services.

3.4.3 Environment Related Factors

The environmental context of the framework refers to the domain where a firm conducts its business and involves its industry, competitors, access to outside resources and is related to government's influence (Tornatzky & Fleischer, 1990). This domain fundamentally infers that adoption of innovative technologies by an organisation is influenced by the environment in which it operates. Environmental factors of the research framework are twofold- pressure from external partners and government policy. The factors within the environment domains are discussed in the following sub-sections.

3.4.3.1 Pressure from External Partners

In many cases, an organisation may adopt a technology due to influences exerted by its business partners. This adoption of a new technology can significantly be influenced by external pressure, particularly when this technology directly affects the competition and is a strategic necessity. In this situation, the pressure to adopt new smart city services quickly is to provide better services and gain strategic advantages. However, the decision to do so may result in an unexpected security concern (AlHogail, 2018). The following hypothesis has been proposed to validate influence of external pressure towards trust:

H4: Perceived external pressure positively influences stakeholders' trust on smart city services.

3.4.3.2 Government Policy

The government policy factor in this context refers to the way governments plan to support the implementation and adoption of innovative technologies in the region. In relation to government policy, Van Zoonen (2019) believes that smart city services need to adhere strictly to existing government policy, as non-compliance may result in additional transaction costs and potential legal outcomes. This is supported by Chang et al. (2006) who found that government policies have a positive impact on organisations trying to adopt new information systems technology. Similarly, Knack and Zak (2003) conclude that not all government policies on public services have influence on trust. Significant positive influence found between any form of government policies towards users' or citizens' trust can justify consideration of government policy in this study to influence stakeholders' trust on the related services. Based on these facts, the following hypothesis has been presented:

H5: Government policies have positive influence towards stakeholders' trust on smart city services.

3.4.4 Security Related Factors

The context of security here refers to the goal to protect information from attacks, viruses, frauds, and various other malicious activities that may cause distress to the information or the infrastructure in the smart cities (Ijaz et al., 2016). Security factors have always been associated with the adoption of innovative technologies such as big data and IoT (Balte et al., 2015; Salleh et al., 2015). Security domain, being the main focus of the research, consists of three factors: perceived privacy; perceived information security, and self-efficacy in information security. The following subsections discuss the factors related to security domain of the theoretical framework of the research.

3.4.4.1 Perceived Privacy

Privacy is the fundamental right of the individual and should be guaranteed by any systems including smart city services. Chourabi et al. (2012) identify privacy and security as influencing factors in the smart city initiative model, where privacy and security factors are related to the built infrastructure domain of the smart city. Privacy challenges in the digital environment are a major threat to the success of initiatives such as e-government because of mistrust and scepticism of such services by citizens (Belanger & Hiller, 2006). Privacy can also play a major role in determining trust by the users or stakeholders of smart cities because smart cities comprise multiple digital services. The following hypothesis is proposed for the privacy factor in this study:

H6: Perceived privacy of the smart city services positively influences stakeholders' trust in smart city services.

3.4.4.2 Perceived Information Security

Perceived information security is defined as the probability by which users or consumers believe that their sensitive information will not be tampered with by either viewing stored data or manipulated during transmission or storage by unauthorised persons, meeting their expectation (Chellappa & Pavlou, 2002). Security has been identified as a factor having significant influence towards the intention to adopt risky technologies that use the internet (Gupta & Xu, 2010). An equivalent scenario of perceived information security in the smart city services would be the extent by which the expectation of users, or city inhabitants, is met to ensure their confidential information is not compromised while in transit or at storage. Chellappa and Pavlou (2002) suggest that online consumers' perception towards information security is determined by the mechanism of robust security technologies such as encryption, protection, verification and authentication. However, perceived information security may be

determined by different factors depending on the information technology environment. There is a strong influence of information security and privacy towards adoption of internet-based services such as internet banking (Lee & Turban, 2001). Goldfinch et al. (2009) find that security of government's electronic services is an important factor towards its adoption by citizens. Hence, it can be generalised that intention to adopt new technology is fairly determined by its end-users' trust over the security and privacy of that technology. It is, however, interesting to know the relationship between the perception of information security and intention to adopt smart city services. Therefore, the hypothesis has been proposed as:

H7*: Perceived information security of the smart city services positively influence stakeholders' trust in smart city services*

3.4.4.3 Self-Efficacy in Information Security

Self-efficacy, being an important paradigm of social cognitive theory, proximally determines individual behaviour (Bandura, 1986). Individuals with a higher level of self-efficacy tend to have better motivation, cognitive resources and ability to mobilise themselves towards successful execution of a task (Stajkovic & Luthans, 1998). Rhee et al. (2009) define self-efficacy in context of information security as a belief in one's capacity to protect information and information systems from unauthorised disclosure, modification, loss, destruction, and lack of availability. However, self-efficacy has been differentiated into various types, such as general computer self-efficacy and specific self-efficacy such as one related to safe and appropriate use of internet transactions (Kim et al., 2009). Self-efficacy of smart city stakeholders therefore is theorised to play a significant role towards trust and indirect role towards intention to adopt smart city services and technologies if stakeholders' trust is derived or influenced by the information security related self-efficacy. A research by Rhee et al. (2009) used six variables such as prior computer/internet experience, security breach

incidents, general controllability, intention to strengthen security effort, technological security practice and behavioural security practice, to study self-efficacy. Rhee et al. (2009) concluded that users' intention to apply security effort is significantly influenced by self-efficacy in information security. Another study by Suki and Ramayah (2010), to identify intention to adopt e-government, has indicated self-efficacy and intention to adopt the government's electronic services as contributing factors along with eight other factors they studied. Self-efficacy therefore is considered as a contributing factor for building stakeholders' trust leading to adoption of smart city services. It may have indirect influence towards intention to adopt, however. The hypothesis to relate information security self-efficacy and trust is proposed as:

H8*: Self-efficacy in information security positively influences stakeholders' trust in smart city services*

3.4.5 Trust in Smart City Services

Information security and trust towards an information system are believed to be inter-related (Chellappa & Pavlou, 2002). Developing trust between smart city services and its users or stakeholders is important as trust plays an important role towards consumer behaviour (Schurr & Ozanne, 1985). Trust also represents the willingness to assume the risk of information disclosure (Mayer et al., 1995). The representation of trust by Koller (1988) as a function of an extent of risk of a certain situation can be alternatively viewed as a function of particular smart service users' risk. This means when there is minimal risk of security in the smart services, there would be more trust towards such service or system. There are many studies that tested relationships between perceived information security and trust. The study of trust-based determinants in the smart city services adoption in the case of smart city services may generate an important outcome by identifying the influencing determinants

towards stakeholders' trust on smart city services and their intention to adopt the smart services derived by this trust. Tolbert and Mossberger (2006) categorise trust in government's electronic services into two categories: process-based trust and institution-based trust. Process-based trust depends on the government's responsiveness via improved communication, online platform's use for increasing access to information, increased citizens' participation and enhanced efficiency and effectiveness to e-government services. Institution based trust is created by transparency, responsibility, increased participation, efficiency and effectiveness of the government's electronic services (Tolbert & Mossberger, 2006). The hypothesis is proposed as follows:

H9: Trust in smart city services and technologies positively influence stakeholders' intention to adopt smart city services and technologies.

Table 3.3 presents research context and the variables used in the technology adoption studies, where trust is considered an important factor in influencing users' decision to adopt new technologies. This study adopted the variables presented in Table 3.3. Technology, organisation and environment dimension are widely used for the study of innovative technologies as shown in the literature Table 3.2. Variables that are added in the security dimension of the research framework are also taken from previous studies that considered perceived information security, perceived privacy and self-efficacy in information security as influencing factors towards technology adoption. The current research assesses how collected data supports the variables used in the research framework.

The proposed theoretical framework of the research is presented in Figure 3.6. A total of nine hypotheses will be tested using Structured Equation Modelling (SEM) Partial Least Square

(PLS), where the structural relationship between dependant and independent variables will be studied by looking at the combined result of factor analysis and multiple regression.

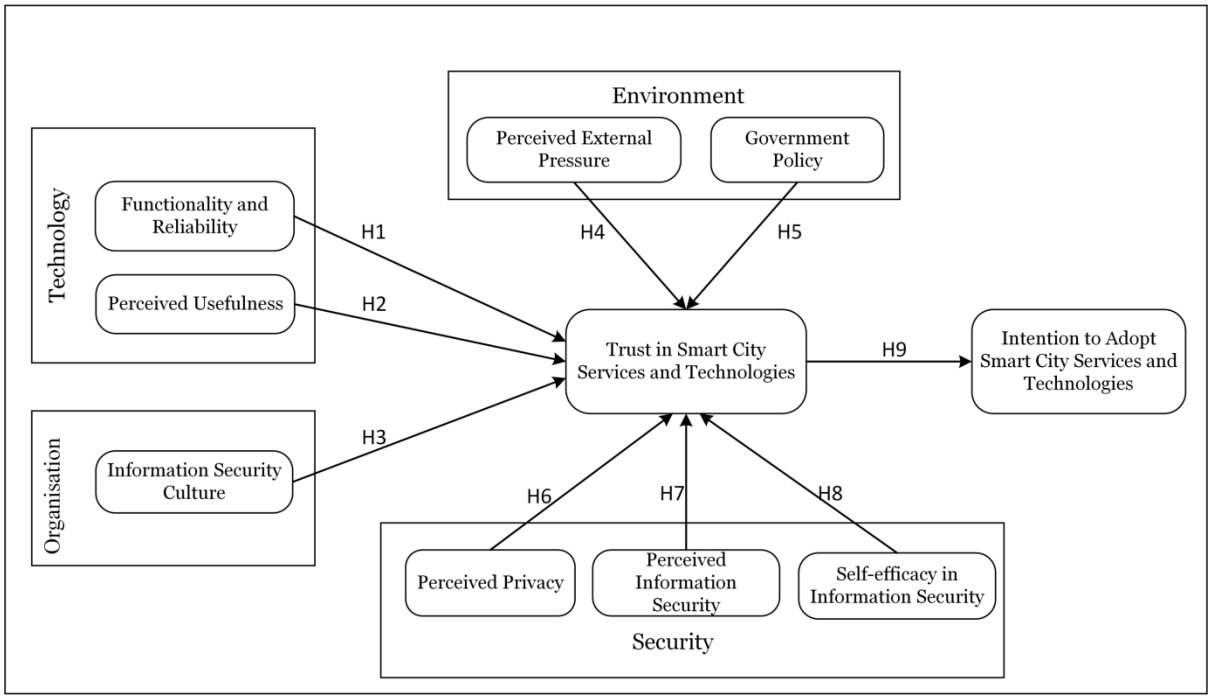


Figure 3.6 Conceptual Framework of the Research

3.5 Conclusion

This chapter has laid the foundation for a proposed framework for the research based on TOE model. There are limited studies on trust-based adoption model of smart city services. The initiation and acceptance of smart city services need to be adopted by its stakeholders for the success of such services. TOE model has been used in the adoption of various ICT based services. This research adds a security dimension to the TOE model to determine security related factors towards stakeholders' trust and intention to adopt smart city services. In other words, the framework proposed in this chapter aims to provide empirical evidence regarding influences of technology, organisation, environment, and security related factors towards

stakeholders' trust and intention to adopt smart city services. The next chapter will discuss methodology, explaining how the proposed framework will be tested.

4 Research Methodology

4.1 Introduction

The aim of this chapter is to provide an overview of the design, methods, sampling, data collection and data analysis approach used in the research. Based on the discussion on various research philosophies and approaches, choices have been made to suit the context of the current research. After introducing the chapter in Section 4.1, Section 4.2 discusses the different research paradigms and explains the paradigm used in this research. Likewise, Sections 4.3 and 4.4 provide overviews of the multiple research methods available, explains why quantitative method has been adopted in this research. The approach towards development of research instrument is also discussed. Next, Section 4.5 explains the data collection and data analysis approaches used. Sections 4.6, 4.7 and 4.8 address sampling approach, ethical issues and scope of the research. Section 4.9 concludes the chapter. The organisation of this chapter is shown in Figure 4.1 below.

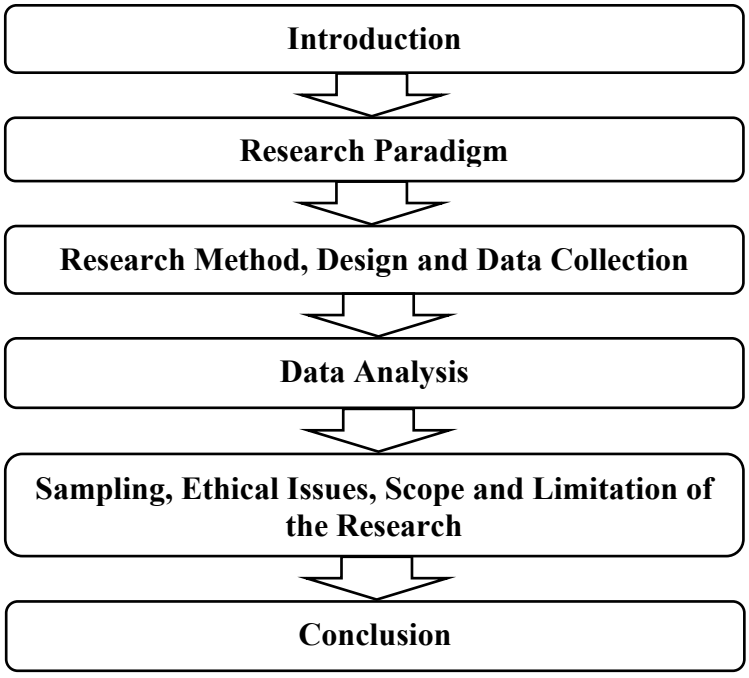


Figure 4.1 Overview of the Chapter 4

4.2 Research Paradigm

Individuals have their own unique views of the world; there are different ways to look into problems and their possible solutions. These individual beliefs are often called paradigms and views towards research problems, and the way to solve research problems, can incorporate a specific paradigm (Sekaran & Bougie, 2016). Guba and Lincoln (1994) and Sekaran and Bougie (2016) present various philosophical viewpoints including positivism, constructivism, critical theory and realism or post positivism. However, the appropriateness of the specific paradigm can be determined by evaluating the characteristics of each paradigm. Realism or post positivism paradigm is regarded suitable for quantitative-qualitative research (Guba & Lincoln, 1994). This paradigm represents both positivist and interpretivist paradigms to prove how those involved attempt to improve their surrounds. However, Hathaway (1995) suggests positivism is concerned more about quantitative research where the research is empirical-analytic in nature. Different varieties of positivism paradigm are indicated by Phillips (1983), one of which is logical positivism.

Logical positivism is also known as objectivist or 'hypothetico-deductive' paradigm. It focuses on phenomena that are objectively determinable and observable. The current research involves stakeholders' view about the technology trust and the role of trust in adopting smart city services. In addition, various factors associated with technology, organisation, environment and security are studied to understand their influence on smart city services adoption. According to Orlikowski and Baroudi (1991), the positivistic view is the dominant one in information system research. In fact, 81% of the published empirical research in this field adopted this paradigm (Chen & Hirschheim, 2004). The nature of this research study is in line with the positivist paradigms.

4.3 Research Method

The most widely used research methods are qualitative, quantitative or a combination of both methods (Saunders et al., 2009). The use of qualitative or quantitative research methods depends on the nature of research problems and both methods have their benefits and pitfalls. Newman et al. (1998) suggest choosing one from various research methods is an individual choice that the researcher makes based on prior assumption, and the rules of procedure, consistent with those assumptions becomes the standard in science. This means no method is superior to another, however one should consider the standard set by prior research studies when adopting a specific research method. While qualitative method such as interview is commonly used to gather subjective knowledge of a research problem (Ranjit, 2011), it is useful in situations where there is a lack of theory behind a research problem, where the available theory is inadequate or biased, when one is trying to describe a subject to develop a theory out of it, or when other methods are more applicable than qualitative method for solving the research problem (Morse, 1991).

The current research study adopts a quantitative research method which is suggested as the most commonly used method of research when there is well established theory to support the research model (Creswell, 2007). Theories related to adoption of technology are analysed to develop a theoretical framework of the research. This makes use of quantitative method an adequate option for this research. One of the most important advantages of using quantitative method is that data can be analysed using quantitative analysis tools and can be easily represented using appropriate figures such as charts or graphs to help explore trends in data and identify relationships between the variables (Saunders et al., 2009). This research aims to identify the perceptions of smart city stakeholders regarding how various factors, including factors related to security, influence stakeholders' trust towards their intention to adopt smart

city related services and technology in regional Queensland cities. For this, a careful selection of participants including smart city stakeholders, is necessary. To obtain an adequate and consolidated outcome of the research, smart city stakeholders such as information technology professionals working in regional Queensland were invited to complete the survey.

4.4 Research Design and Data Collection

After making the decision on which research method to use for the study, comes the stage of planning or designing the study (Creswell, 2009). Research design 'Survey Research' is an umbrella term which has a variety of different methods and tools in order to gather information (Andres, 2012). The different formats involved in this umbrella term are self-administered survey, group-administered survey, mail survey, diaries, online survey, email survey, web survey, interviewer-administered survey, telephone survey and face-to-face interviews (Andres, 2012). Survey using questionnaire has been adopted for this research as survey is a convenient way to obtain views and adopting this method is believed to be convenient for the participants as it provides quick turnaround for data collection (Creswell, 2007). For the convenience of participants as well as researcher, an online survey was selected as an appropriate data collection method for this research.

This study adopts the questionnaire from previous studies conducted in a similar context. The earlier studies used innovation adoption or smart technology adoption as their research context. Churchill (1979) provided a detailed procedure for measure development. In fact, the procedure has been adopted by many studies because of its effectiveness in achieving appropriate measures. Hence, this study makes use of the proven steps detailed below.

The steps followed for the questionnaire involved specifying the domain of constructs, generating sample items, expert review and final approval. The domain specification for the survey was discussed in Chapter 3 where, a number of theories used in the study of technology adoption were discussed and use of TOE model was justified. With security dimension added to existing TOE dimensions, the domain of the constructs are technology, organisation, environment and security and variables within each domain are presented in Table 3.4 of Section 3.4. The sample items generation is shown in Table 4.1. The sample items or indicators used for each variable are adopted from prior studies that used the same variables under a similar study context. After sample generation, expert review was sought to evaluate adequacy of the selected indicators. After the approval from experts, the questionnaire items were finally approved for the data collection. The figure 4.2 shows the questionnaire development process used in this study.

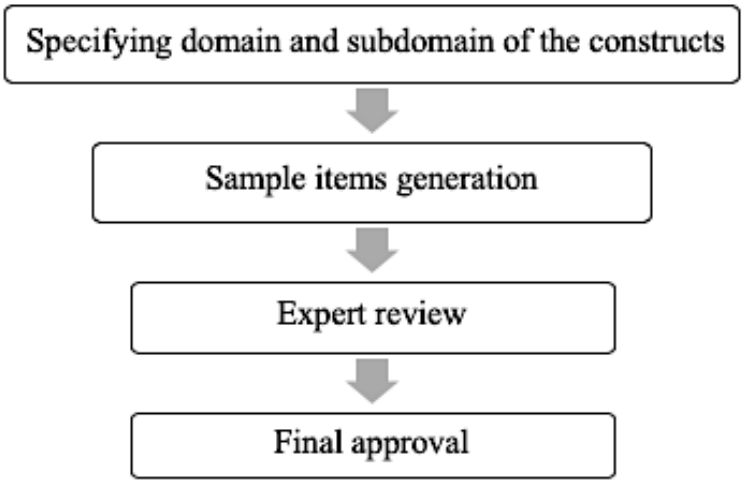


Figure 4.2 Process for Questionnaire Development

The questionnaire (Appendix B) was developed based on the conceptual framework of the research as shown in Figure 3.6, where each item was taken from previous survey-based

studies to ensure reliability of the indicators. The indicator source matric is provided in Table 4.1 below.

Table 4.1 Indicators Source Matrix (Sample Items)

Constructs	**Indicators**	**Sources**
Perceived Usefulness	Will not create harassment. Services are convenience. Services give greater control. Improves the efficiency of obtaining services.	Kim et al., (2007); Li et al. (2018); Rhee et al. (2009)
Functionality and Reliability	Technical capacity to ensure data will not be intercepted by hackers. Sufficient technical capacity to ensure data cannot be modified by a third party.	Alharbi et al. (2017)
Information Security Culture	Familiarity with the information security policies of organisation. Individual's role for escalating information security incidents. Awareness of the information security responsibilities	Alnatheer (2012); Chaula (2006); Kruger and Kearney (2006)
Perceived External Pressure	Smart city services are effective way to interact with government. Use of smart services will improve the efficiency of obtaining services.	Li et al. (2018); Rhee et al. (2009)
Government Policy	Smart city services are effective way to interact with government. Use of smart services will improve the efficiency of obtaining services.	Li et al. (2018); Rhee et al. (2009)
Perceived Privacy	There will be no loss of data from an agency behaving opportunistically in smart city services. Feel safe when I send personal information to councils. Feel confident about privacy with regards to the smart city services.	Carter and McBride (2010); Flavián and Guinalíu (2006); Sarabdeen et al. (2014)
Perceived Information Security	Smart services provided are reliable. Council shows concern for the privacy of its users. Information I provide to council will not be manipulated. Transaction is secure while using the smart services.	Alharbi et al. (2017); Sarabdeen et al. (2014)

Self-Efficacy in Information Security	Confidence in handling virus infected files. Confidence in understanding terms relating to information security. Confidence in learning the method to protect information and information system. Confidence in managing files in computer. Confidence in setting the Web browser to different security levels. Confidence in using different programs to protect my information and information system. Confidence in updating security patches to the operating system. Confidence in following the 'user guide' when help is needed to protect my information and information system.	Rhee et al. (2009)
Trust	Councils and other relevant authorities can be trusted to carry out online transactions faithfully. Legal and technological structures adequately protect from problems on the internet. Smart city services would provide a valuable service for residents in our city council. The responsible firm providing the smart city services will take full responsibility for any type of insecurity.	Alharbi et al. (2017); Alsaghier (2009); Rhee et al. (2009);
Intention to Adopt	Confidence in the technology used in smart city's services. Not concerned that the information submitted online could be misused. Believe that smart city services are safe to interact with for financial purposes.	Alharbi et al. (2017); Alsaghier (2009); Shin (2010);

Survey using questionnaire being a quantitative method, is utilised in collecting statistics (Burns & Grove, 2005), where being able to convert the questionnaire into numeric data enables quantitative analysis of the data. Brace (2018) suggests questionnaire is an important tool to elicit information, helping the researcher to answer the research questions only if designed in a proper way, because a poorly designed questionnaire not only limits the required data but may also involve inaccurate data in research. Despite being a very popular

tool for quantitative research, a survey using questionnaire has some disadvantages as well. Thompson and Surface (2007) argue that survey questionnaires have high possibility to be left incomplete or will not be returned to researchers because (a) respondents are too busy, (b) researchers have not designed the questionnaire appropriately or (c) the result of the study is not important to the respondent, or respondents do not want to waste time filling in a survey questionnaire that is not important to them. Thus, low response rate of the survey is regarded as a major disadvantage of using survey method while consistency of data is the positive side of using this survey method.

For the purpose of the research, an email with an online survey link was sent to nine organisations, including at least six councils in regional Queensland, to an ICT professionals' network in central Queensland and to several ICT professionals working in the central Queensland region. Recipients were asked to complete the survey and forward the email to all other eligible respondents in their network. The initial contact acts as a 'seed' in the referral sampling. Referral, as well as purposive sampling, which falls under the snowball sampling, was the most reliable method to involve the most eligible participants in the study (Saunders et al., 2009). A five-scale 'Likert' questionnaire was used, with a few open-ended questions to offer respondents an opportunity to make further comments. The time taken to complete the survey was between 13 and 20 minutes. Numeric data generated from the survey was easy to analyse using statistical analysis tools such as IBM SPSS and SmartPLS.

4.5 Data Analysis

The data analysis involves three stages: (a) data screening and cleaning, (b) measurement model validation, and (c) structural model evaluation. The data screening procedure involves visual inspection of data to identify missing values and errors, and also the test of normality

to see if data meets the statistical assumptions (Hair et al., 2016). For the data screening process, IBM SPSS Statistics version 21 was used and SmartPLS 2.0 (Ringle et al., 2005) was used for the Structural Equation Modelling (SEM) Path Modelling (PM). The following sections define and explain the measures used for quantitative data analysis in this research.

4.5.1 Structural Equation Modelling

Structural equation modelling (SEM) has been described as a combination of several statistical analysis approaches such as factor analysis, multiple regression analysis, correlation analysis, discriminant analysis and variance analysis (Ullman, 2001). SEM is more useful for confirmatory data analysis than exploratory. The advantage of using SEM is it also provides the relationships among the latent variables incorporating two components such as measurement model and structural model (Schreiber et al., 2006). Apart from being suitable for confirmatory factor analysis, SEM has added benefits such as estimation of error variance parameters, it can analyse both latent and observed variables, and there is no widely used alternative for multivariate relationship modelling (Byrne, 2013). SEM is relatively new but is a sophisticated data analysis method concerned with relationships between a set of variables (Pallant, 2013). A theory proposed in the form of relationship between the measured variables and latent constructs can be validated using SEM by looking at how well the theory is supported by the data (Hair et al., 2010). Two approaches are suggested in performing SEM, which are measurement model and structural model (Anderson & Gerbing, 1988). In measurement model, all the individual items, variables or observations are evaluated to ensure the appropriateness of the construct. This model helps to specify the hypothetical relationship between the latent variables. After achieving measure of the constructs by measurement model, relationship between the constructs is explored by structural model.

Two distinct methods can be applied for SEM. The first method is maximum likelihood estimation or covariance-based SEM (CB-SEM) and the second method is PLS, which is also known as component based or variance-based approach (Hair et al., 2010). CB-SEM focuses on overall fit between the estimated covariance model with the calculated covariance matrix with the help of maximum likelihood estimation (Gefen et al., 2000). CB-SEM is mostly used for the purpose of testing and development of theory, where Partial Least Square is used to see if the relationships between variables are significant through ordinary least square estimation (Gefen et al., 2000). There are few criteria for using CB-SEM, regardless of its popularity, such as normality assumption should be met beforehand, and dataset used should be large enough. Also, it is important for a user to be cautious, whether their model specification is formative or reflective, as this is the common mis-specification users encounter in SEM (Albers, 2010). There are statistical software options available for SEM such as SmartPLS, AMOS (Analysis of Moment Structure), LISREL (Linear Structural Relations) and EQS (Equations). IBM SPSS version 26 and SmartPLS 2.0 were used in this research for analysing descriptive statistics and structural equation modelling. The advantage of using SmartPLS is its users are able to create, modify and run the path diagrams using graphical user interface (Ringle et al., 2005).

4.5.2 Partial Least Square Path Modelling

Partial Least Square (PLS), also known as Partial Least Square Structural Equation Modelling (PLS-SEM) has been a widely used method as a component-based estimation method (Hair et al., 2010). Different valid explanations are made by various authors regarding why PLS is an appropriate technique for data analysis as it is widely used in multiple disciplines (Ismail et al., 2013). SEM works with a number of related equations

simultaneously and has some advantages over other familiar methods, therefore presenting as a general method for linear modelling (Monecke & Leisch, 2012). Originally developed by Wold (1966) and Lohmöller (1989), the approach of partial least square to SEM provides an alternative of more prominent co-variance-based SEM. In fact, a comparative study between CB-SEM and PLS-SEM by Thomas et al. (2005) and Astrachan et al. (2014) suggest PLS-SEM is beneficial over covariance-based methods.

There are two primary advantages reported for using PLS-SEM over CB-SEM. Firstly, PLS-SEM can easily estimate more complex models with lower sample sizes. Complexity of the model is described by Hair et al. (2010) and Chin (1998) as having multiple dependent and independent variables and relationships between those variables. Secondly, PLS-SEM provides relaxation on hard distributional assumptions, usually expected by maximum likelihood approach used to estimate models in CB-SEM (Astrachan et al., 2014). The research model presented in this study consists of several variables and this study attempts to study the relationships between the observed data and the latent variables, and the relationships between the latent variables. Hence the presented model is considered complex. Chin (1998) argues that PLS path modelling technique is more appropriate depending on the nature of objectives, alignment of data to theory, properties of data and level of theoretical knowledge and measurement development. The PLS-SEM method also allows estimating the cause-effect relationship models with latent variables. It consists of two sub-models: the measurement model and structural model. The measurement model helps to understand the relationships between the observed data and the latent variables whereas, the structural model helps to understand the relationships between the latent variables (Byrne, 2013; Schreiber et al., 2006). Hence, this study adopted the PLS-SEM method to study the relationships between the observed data and the latent variables, and the relationships between the latent variables.

This study developed a theoretical framework on the basis of theories and prior literature, and data was collected by the use of survey questionnaire. Having a sound theoretical basis of proposed factors fulfils the criteria of Chin (1998) to use PLS path modelling as the best data analysis tool for this research. Also, PLS is the best approach to understand and explain complex models where multiple relationships among the variables are evaluated. Only reflective constructs are used in the model specification because use of CB-SEM assumes all measures as reflective only (Chin, 2010). The next section will explain reflective versus formative measurement models.

4.5.3 Construct Specification: Reflective and Formative

Reflective and formative specification has not been specified appropriately by many prior studies, which can result towards bias in estimating relationship structure (Jarvis et al., 2003). SEM related literature indicate latent variables can be specified using reflective or formative constructs. The nature of the reflective and formative measurement models is described by Coltman et al., (2008), Chin (2010) and Hair et al. (2010). Reflective indicators reflect the same underlying construct and they are expected to have higher correlations and to flow from construct to indicators. The reflective indicators are also interchangeable and eliminating an indicator from the model does not usually change the theme of the construct. Conversely, the formative model consists of composite latent variables, where causation flows from the indicators to the construct being measured and the indicators should not have high correlations (Jarvis et al., 2003). The natures of reflective and formative models are represented in Figure 4.3.

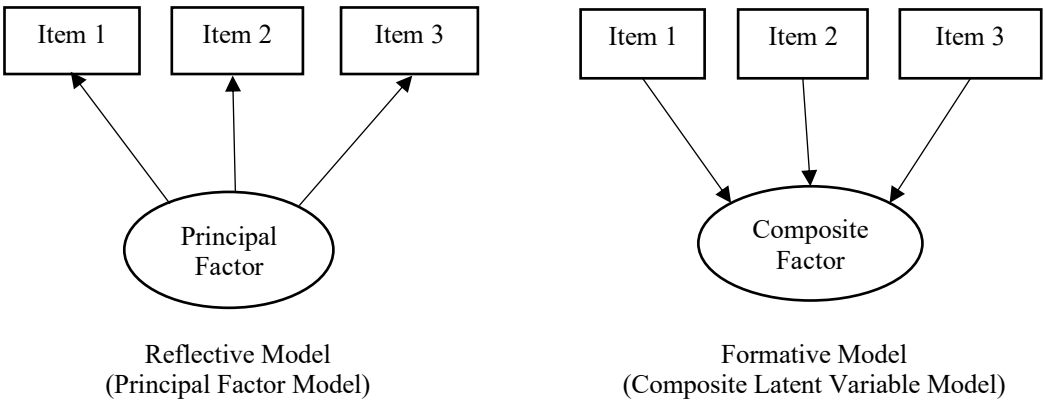
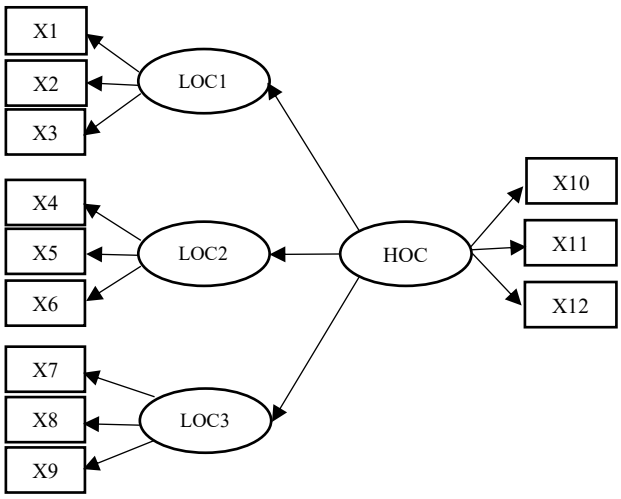
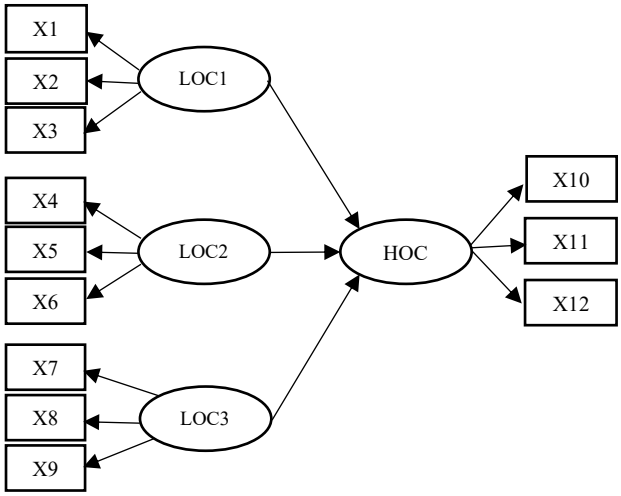


Figure 4.3 Nature of Reflective and Formative Measurement Models

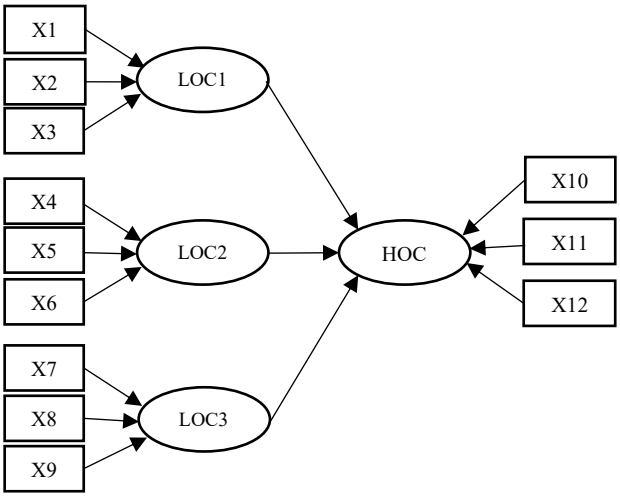
Four different types of hierarchical component models are indicated by Ringle et al., (2012) and Jarvis et al. (2003) in relation to the order of the components used. Different sub-types of measurement models are reflective-reflective, reflective-formative, formative-formative and formative-reflective models, which are presented in Figure 4.4. The hierarchical model involves indicators, low order constructs (LOC) and higher order constructs (HOC). Types of these models are based on reflective and formative nature of relationship between indicators and low order constructs and between low order constructs and high order constructs. This research study does not consist of low order and high order constructs, rather there are several indicators for each factor. However, the measurement model includes causal relationships between independent factors and dependent factors. The measurement model developed for this study involves reflective relationships between indicators and independent factors and formative relationships between dependent and independent factors.



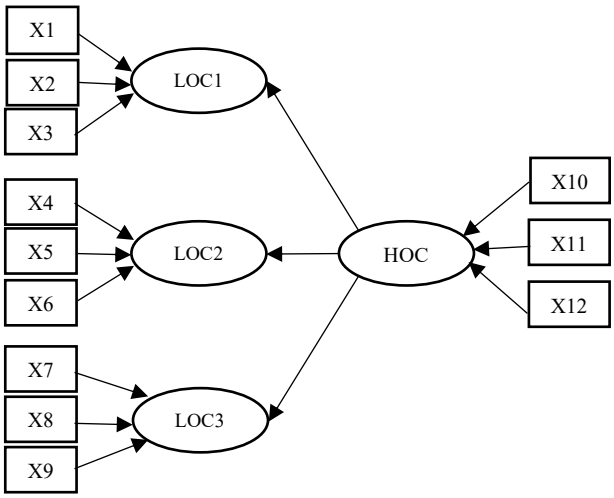
Type 1: Reflective-Reflective



Type 2: Reflective-Formative



Type 3: Formative-Formative



Type 4: Formative-Reflective

Note: LOC – Low Order Construct, HOC – High order construct, X(1-12) – Indicators

Figure 4.4 Types of Hierarchical Component Models

Source: Becker, Klein and Wetzels (2012)

4.6 Sampling

Sampling is usually understood as a technique to select a few (sample) from the large group (population) (Ranjit, 2011). The author distinguishes sampling into probability/random, non-probability/non-random and 'mixed' sampling where random sampling is further categorised into simple, stratified and cluster sampling, and non-probability sampling is further categorised into quota, judgmental, accidental, snowball and expert sampling. The mixed sampling method involves systematic sampling method that may involve more than one sampling technique in order to collect different types of data.

The interpretation and estimation of research results are determined by sample size (Hair et al., 2010). The sample size of 200 is recommended to be appropriate for structural models such as Structural Equation Modelling (SEM) (MacCallum et al., 1996). Loehlin (1992) also supports at least 200 sample sizes for testing structural models at 95% confidence interval. Although there is a strong correlation between size of sample and statistical power of covariance structure model (SEM), no globally accepted rule is available regarding sample size for hypothesis testing using structural models (Dolnicar, 2002). Having a larger sample size is important for SEM as a smaller sample size is likely to generate an unreliable statistical outcome while having a larger sample size may minimise the variability and produce stability in the model complexity (Hair et al., 2010). The authors suggested that, depending on the complexity of the measurement model characteristics, 100-400 sample size is regarded as appropriate. Hair et al. (2010) argue that sample size should not be below 100 for factor analysis. The sample size used in this study is 225, which satisfies various suggestions for sample size requirement for the SEM.

Snowball sampling technique was applied to fulfil the required sample size within the available time frame. Snowball sampling is useful where respondents' referral is needed to find more eligible respondents for the survey (Saunders et al., 2009). It was requested in the survey email to forward the email with survey link to any ICT employees working in regional Queensland or associated with regional Queensland. Snowball sampling provides a higher chance for survey requests to reach more eligible respondents and can acquire expected responses in a reasonable time period. A total of 735 emails were sent to various organisations employing ICT professionals in the central Queensland region. A total of 229 responses were received, where four responses were found to be less than 10% completed. Incomplete samples do not provide any details relating to the variables being tested so those four samples were excluded from the final analysis. Response rate of the survey has been calculated as 30.6% (229 responses) which is justifiable in online survey. An analysis of different response rates of the paper-based and online surveys by Nulty (2008) reports relatively lower response rate of online survey than paper-based surveys, where on average 33% and 56% response rate was reported for online and paper-based surveys respectively. The achieved response rate in this study is in line with the reported response rate in the study of Nulty (2008). Furthermore, total responses obtained in this research, which is 229, is acceptable because a sample size of 200 is recommended to be appropriate for structural models such as Structural Equation Modelling (SEM) (Hair et al., 2010; MacCallum et al., 1996). Loehlin (1992) also supports at least 200 sample size for testing structural models at 95% confidence interval. The final sample consists of a total of 225 valid responses. The sample size is considered appropriate for PLS-SEM analysis as per the suggestions made by MacCallum et al. (1996), Loehlin (1992) and Hair et al. (2010).

This research study requires stakeholders who are expected to have better understanding of smart cities to provide their views on the security aspects of smart cities. Only information technology professionals working in regional Queensland were invited to participate. It is assumed that ICT professionals have better knowledge of smart city technologies and may also have better perception about the existing smart city security issues. The smart city stakeholder model used by Khan et al. (2014) identifies smart city stakeholders as: service customers, domain experts, standard governing bodies, legitimate service providers, untrusted service providers, ICT experts, and data custodians.

Ranjit (2011) explains that expert sampling can be adapted in quantitative study, where sample size depends on a researcher's decision without considering the saturation point. Having different sampling options for the data collection, purposive sampling with expert sampling is deemed suitable towards fulfilling the research aim. The data collection method involved survey using questionnaire based on voluntary participation. The sample size surpassed the previously expected 200, totalling 225 valid responses from ICT employees working in various organisations in regional Queensland.

Popescul and Radu (2016) explain that smart city stakeholders associated with cyber security of smart city to be city authority, application developers, service providers and security solutions providers, and they have better understanding of different aspects of smart city related technologies and services. Stakeholders of the smart cities are those who are directly or indirectly involved in strategic and managerial roles in smart regional councils as well as professionals who work in information technology areas. Queensland is the second largest state of Australia by area, and it has a significant number of regional cities and towns. The Australian Government's cities and suburb plan (Australian Government, 2018) suggests that

there are a number of smart city projects under development and some are being developed in Queensland. These smart city projects include smart parking, automated traffic management, smart precinct and digital parking permits. Having a number of smart cities plans in progress, together with governmental intention to support future innovative technology and services deployment in regional cities, Queensland is a suitable study context to assess smart city services adoption. A future research may extend the context to other states.

4.7 Ethical Issues

This research study involves collection of data from human subjects. In the due course of research, individual identifiable data such as questionnaire responses, data files and spreadsheets involving personal emails were generated. Proper management of such data is very crucial for conducting ethical research. Ethics clearance was obtained from CQUniversity Human Research Ethics Committee (CQUHREC) prior to the collection of data. The ethics clearance number for this research is 21284.

To overcome any ethical issues, participants are not identified by any personal identification information such as name, employer, address or any other details that may identify them. The data was kept in university cloud storage, protected securely by the university, and back-up copies were stored in an external storage device and were password protected (encrypted) so data was not accessible by any other person in the event of the device being lost or stolen. All data storage locations were accessible by student researcher supervisors. The participants were given a choice to withdraw their participation from the research at any time before the submission of thesis or publication of results. In this way, ethical issues were addressed and eliminated by following the strict guideline of the CQUHREC.

4.8 Scope of the Research

The research has determined the influence of various factors towards stakeholder trust in smart city services and technologies and whether trust influences the intention to adopt smart city services and technologies. The scope of the research may expand as per the data, but the research is mainly concerned with how technology, organisation, environment and security related factors influence trust towards stakeholder's intention to adopt related technologies and services that enable smart city.

4.9 Conclusion

This chapter has presented the overview of the research design, methods, sampling, data collection, analysis and expected outcome of the research. The detailed strategy has been presented to identify the stakeholders' intention to adopt smart city services in regional Australian cities and councils. The constructs identified by literature review were used to develop the survey questionnaire. A survey is regarded as the best tool to fulfil the research objectives, and a quantitative data analysis method that is SEM, path analysis and confirmatory factor analysis using SmartPLS was selected to analyse the survey data.

5 Data Preparation and Analysis

5.1 Introduction

This chapter details the techniques used for preparing the data for validation and further analysis. Section 5.2 outlines the data preparation. Section 5.3 describes the profiles of respondents. Section 5.4 discusses the construct operationalisation and Section 5.5 discusses preliminary analysis of the data, where data cleansing process is presented. Instrument validation and measurement models are presented in Section 5.6. Further, Sections 5.7 details the structural model examination and Section 5.8 summarises the hypothesis test results. Finally, Section 5.9 concludes the chapter. Figure 5.1 below summarises Chapter 5.

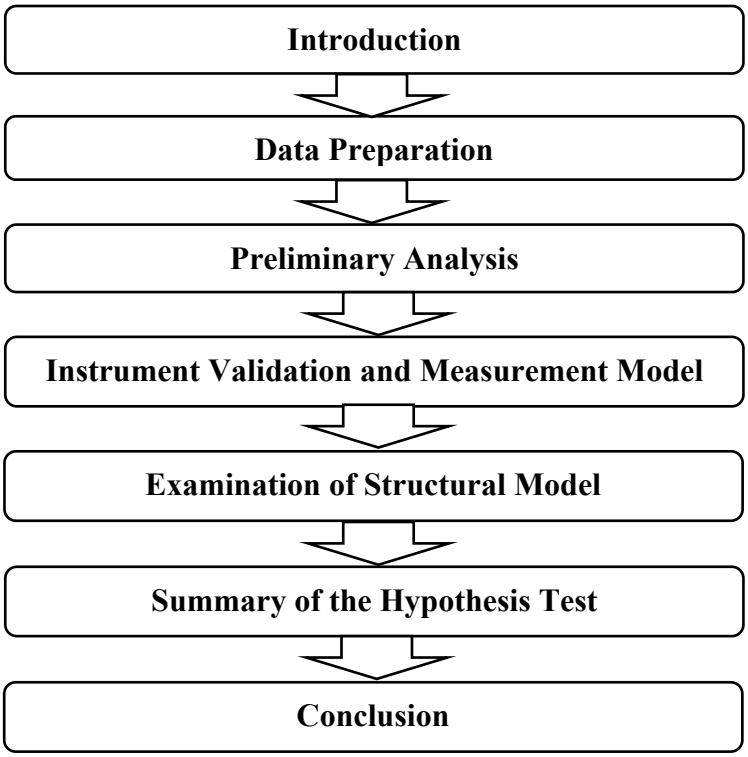


Figure 5.1 Overview of Chapter 5

5.2 Data Preparation

Prior to research instrument validation and conducting multivariate analysis with structural equation modelling, the dataset was prepared and examined. There are multiple reasons why data needs to be examined and prepared beforehand. The two most important reasons for examining and preparing the data beforehand are to minimise the potential measurement errors and to verify that data satisfies the requirements for multivariate analysis (Hair et al., 2010). Multivariate analysis is comprised of a number of statistical techniques used to simultaneously analyse multiple variables and it allows better insight into data generating more knowledge in comparison to bivariate and univariate predecessors (Hair et al., 2006).

5.3 Respondents' Profiles

There were 225 valid responses. Of these, 36% survey respondents were female and 62% were male with 81 and 140 responses from each gender. There were four missing entries for gender, that accounts for the remaining 2% of the total responses. The disparity in the number of male and female respondents may indicate male predominance in the technology sector. Table 5.1 shows the gender of the participants.

Table 5.1 Gender of the Participants

	Male	**Female**	**Missing**	**Total**
Frequency	140	81	4	225
%	62%	36%	2%	100%

A question was asked to specify to which domain individual respondents related. The descriptive analysis of the data shows the majority of the respondents were engaged in business process, followed by education and training with 54 respondents, and technology roles with 45 respondents. Similarly, there were 30, 15, 13 and two respondents from

research and development, consulting, leadership and other domains respectively. Figure 5.2 presents the job profile of the respondents.

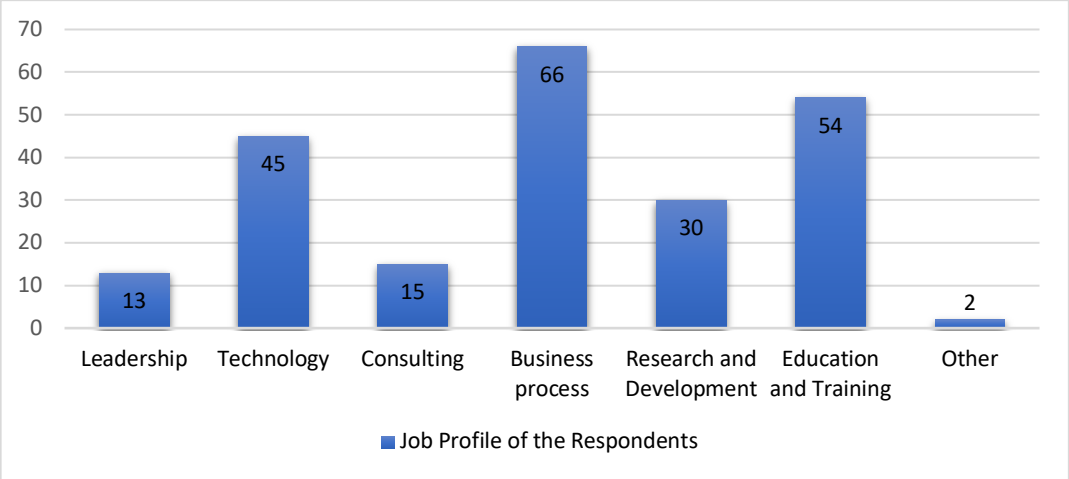


Figure 5.2 Job Profile of the Respondents

Age group analysis shows that the majority of respondents were between of 25 to 54 with 163 respondents from that age range. There were almost 13% respondents aged 18 to 24, 10% from 55 to 64 and 4.4% of respondents were above 65. This indicates there are mostly younger people engaged in ICT roles in regional Queensland. Figure 5.3 shows the age group of the respondents.

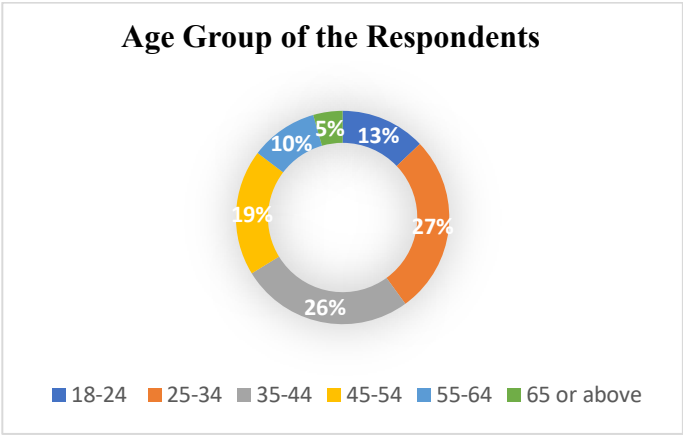


Figure 5.3 Age Group of the Respondents

Most respondents were from the Rockhampton region, accounting for almost 41% of respondents. Others were from Livingstone Shire, Mackay and Townsville regions with 12.4%, 12.9% and 10.7% respectively. Fewer than 5% of respondents were from Cairns, Gladstone, Bundaberg and other councils. A total of 3.1% of respondents declined to identify their local council. Hence, the survey involves responses from a majority of regional Queensland cities and councils. Table 5.2 shows the frequency and percentage of responses by various city councils.

Table 5.2 Frequency and Percentage of Responses by City Council

Council Name	Frequency	Percentage
Rockhampton	92	40.9
Livingstone Shire Council	28	12.4
Mackay	29	12.9
Townsville	24	10.7
Cairns	11	4.9
Gladstone	7	3.1
Bundaberg	7	3.1
Toowoomba	11	4.9
Others	16	7.1
Total	225	100

The respondents had relatively good experience in ICT related fields. The data indicates about 85% of respondents had more than two years of ICT related job experience, while only 35 respondents were relatively new to the field. The high number of well experienced ICT employees involved in the survey suggests the survey was well received by experienced ICT professionals. Table 5.3 shows the ICT related experience of respondents.

Table 5.3 ICT Related Experience of Respondents

ICT Related Experience	Frequency	Percentage
Less than 2 years	35	15.6
2 to 5 years	63	28.0
5 to 10 years	63	28.0
More than 10 years	64	28.4
Total	**225**	**100.0**

5.4 Construct Operationalisation

Conceptual framework of the research is discussed in Chapter 3, where dimensions and constructs are defined and justified to fit in the research framework. The constructs and items used to measure each construct were given unique codes to represent them in the data analysis process. Table 5.4 presents the constructs and items associated with each construct with a code given to them.

Table 5.4 Constructs Operationalisation

Dimension	Constructs	Code for Construct	Code for Indicators
Technology	Perceived Usefulness	T_PU	T_PU1, T_PU2, T_PU3
	Functionality and reliability	T_FR	T_FR1, T_FR2
Organisation	Security culture	O_ISC	O_ISC1, O_ISC2, O_ISC3
Environment	Government Policy	O_GP	O_GP1, O_GP2
	Pressure from external partners	E_PEP	E_PEP1, E_PEP2
Security	Self-efficacy in Information security	S_SEIS	S_SEIS1, S_SEIS2, S_SEIS3, S_SEIS4, S_SEIS5, S_SEIS6, S_SEIS7, S_SEIS8,
	Perceived Privacy	S_PP	S_PP1, S_PP2, S_PP3,
	Perceived Security	S_PS	S_PS1, S_PS1, S_PS1, S_PS4
	Trust	TRUST	TRU1, TRU2, TRU3, TRU4
	Intention to adopt	INTENT	INT_1, INT2, INT3

5.5 Preliminary Analysis

There were four steps to be completed for data preparation. First, the data was imported from the online survey website 'SurveyMonkey' in the SPSS file format. Being able to import data in the SPSS supported format is a time-saving process as the imported data can be opened in the SPSS software package and data cleansing is performed. Survey items were re-coded by numbering them sequentially and checking for any inconsistencies. Next, missing values were analysed to detect any incomplete entries. There is no strong reasoning found in the literature that supports replacing missing values for the entries that are significantly incomplete. The initial sample size was 229. However, during the data cleaning process four responses were deleted as these were less than 10% complete. Moreover, they do not shed light on any of the variables being tested in the proposed research framework. Hence, the final sample consists of 225 responses. Also, normality of the data was tested along with outliers and multicollinearity identification. Finally, non-response bias estimation test was conducted to confirm that collected data characterises the generalised population. The steps followed for the data cleaning are presented in Figure 5.4 below.

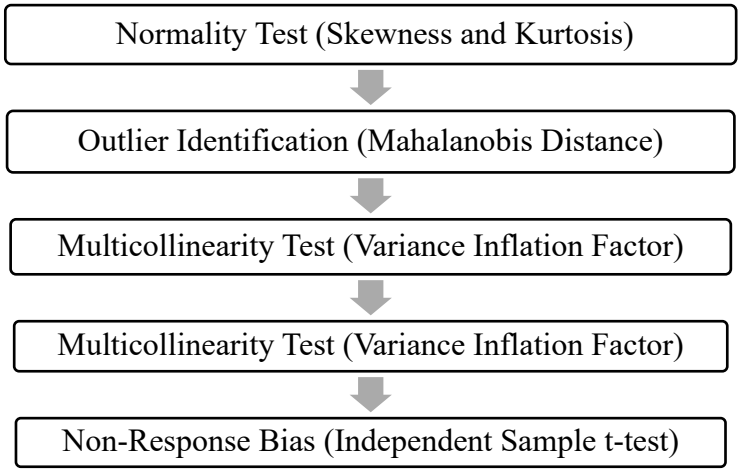


Figure 5.4 Data Cleaning Process Used

5.5.1 Normality Test

Normality indicates whether data is distributed normally. The normal distribution standard form is the one with 1 standard deviation and 0 mean value, which generates a symmetric bell shape plot in a graph. Hair et al. (2006) indicate normality as one of the main assumptions made for the multivariate data analysis. Some of the common statistics that measure distribution of the data are kurtosis, skewness and their standard errors.

Table 5.5 presents normality test results for all the items. Lewis-Beck et al. (2004) indicate that skewness and kurtosis values should be within the range of -1 to +1 and -2 to +2 respectively. Further, Tabachnick and Fidell (2001) indicate skewness and kurtosis value within the range of -4 to +4 is acceptable.

Table 5.5 Normal Distribution Test Results

Item	Mean	S.D.	Skewness	Kurtosis	Item	Mean	S.D.	Skewness	Kurtosis
T_PU_1	3.43	0.87	-0.70	0.05	S_PP_2	3.00	0.62	0.23	0.34
T_PU_2	4.25	0.58	-0.38	0.95	S_PP_3	3.14	0.75	-0.10	-0.21
T_PU_3	3.84	0.83	-0.31	-0.46	S_SEIS_1	3.77	0.69	-1.35	2.25
T_FR_1	3.24	0.76	-0.14	-0.75	S_SEIS_2	3.52	0.86	-0.62	-0.36
T_FR_2	3.24	0.78	-0.38	-0.26	S_ SEIS _3	3.35	0.85	-0.22	-0.64
O_ISC_1	3.68	0.75	-0.63	0.58	S_ SEIS _4	3.59	0.87	-0.59	-0.27
O_ISC_2	3.84	0.83	-0.45	0.01	S_ SEIS _5	3.20	0.82	-0.18	-1.13
O_ISC_3	3.60	0.75	-0.55	-0.02	S_ SEIS _6	3.12	0.92	-0.14	-0.84
E_PEP_1	4.10	0.76	-0.41	-0.47	S_ SEIS _7	3.15	0.93	-0.11	-0.76
E_PEP_2	4.33	0.65	-0.65	0.29	S_ SEIS _8	3.43	0.83	-0.60	-0.05
E_GP_1	4.29	0.75	-1.50	3.74	TRU_1	4.48	0.56	-0.44	-0.84
E_GP_2	4.06	0.83	-0.88	0.83	TRU_2	3.29	0.65	-0.07	-0.32
S_PS_1	3.04	0.56	-0.29	1.39	TRU_3	3.38	0.88	-0.35	-0.41
S_PS_2	3.03	0.82	-0.10	-0.64	TRU_4	3.67	0.97	-0.67	-0.12
S_PS_3	3.35	0.61	-0.23	-0.53	INTENT_1	3.46	0.67	-0.52	-0.32
S_PS_4	3.25	0.68	0.08	-0.17	INTENT_2	3.00	0.74	0.13	-0.47
S_PP_1	2.20	0.97	0.62	-0.14	INTENT_3	2.44	0.83	0.57	-0.13

The results presented in Table 5.5 indicate that both skewness and kurtosis values are within the range but the item E_GP_1 and the item (S_SEIS_1) 'I feel confident handling virus infected files', when referring to Lewis-Beck et al. (2004) show high skewness and kurtosis. However, all values are accepted to be within the normal range of -4 to +4 as supported by Tabachnick and Fidell (2001).

5.5.2 Outliers Identification

Outlier identification is an examination of observations with extreme values, so that they can be eliminated from the analysis as they may influence the multivariate analysis if not deleted (Hair et al., 2014). Outliers can be identified by using SPSS outlier report, which is also a convenient method for this analysis. As 5-scale Likert data is used, multivariate outlier was regarded useful as univariate outlier identification was inappropriate. For univariate outlier, Q-Q plot, histogram, steam-leaf diagram can be visually inspected, or SPSS outlier report can be used to identify outliers. For multivariate outlier detection, widely used approaches are to use Mahalanobis distance (Tabachnick & Fidell, 2007) and Cook's distance (Cook & Weisberg, 1982). However, a comparative study of various outlier detection procedures in multiple linear regression suggested Mahalanobis distance is preferred method over Cook's distance in the studies with lower samples (Oyeyemi et al., 2015).

The multivariate outlier was identified by calculating Mahalanobis distance (D^2) divided by degree of freedom (df) (number of items in this case) for each construct individually. There is no strict guideline regarding the threshold for D^2/df, however, Hair et al. (2014) recommend the threshold value of 2.5 for small samples (sample size below 80) and up to 4.0 for larger samples is accepted. The results showed all instances had D^2/df values below 4.0. Therefore, no multivariate outlier was identified in the data.

5.5.3 Multicollinearity

Multicollinearity exists when there are multiple independent variables measuring the same thing. Multicollinearity is related to the measure of extent to which a variable's effect is predicted for by another variable (Hair et al., 2014). Firstly, initial evaluation of multicollinearity is done by looking at item-to-item correlation matrix (Appendix A). Even though some correlation is expected between the items from the same variable, higher than 0.9 correlation between any two items may cause a statistical problem (Tabachnick & Fidell, 2007). No higher correlation between items has been observed in the correlation matrix.

Secondly, another widely used approach to evaluate multicollinearity is through variance inflation factor (VIF). VIF is the degree by which an indicator's variance is explained by another indicator of the same construct (Urbach & Ahlemann, 2010). Hair et al. (2014) suggest VIF values higher than 5.0 implies high collinearity. The VIF and tolerance values for each item are listed in Table 5.6. VIF valued obtained from SmartPLS version 3.2.7 for all constructs shows no values higher than 5.0. Moreover, the observed results showed five items with VIF between 2.0 and 2.5 and all other items had VIF less than 2.0. Therefore, no multicollinearity was observed as per the threshold suggested by Hair et al. (2014).

Table 5.6 Variance Inflation Factor (VIF) and Tolerance

Items	VIF	Tolerance (1/VIF)	Items	VIF	Tolerance (1/VIF)
T_PU_1	1.22	0.82	S_PS_3	1.41	0.71
T_PU_2	1.25	0.80	S_PS_4	1.23	0.81
T_PU_3	1.36	0.73	S_SEIS_1	1.20	0.83
T_FR_1	1.59	0.63	S_SEIS_2	2.00	0.50
T_FR_2	1.59	0.63	S_SEIS_3	2.47	0.40
O_ISC_1	1.50	0.67	S_SEIS_4	2.10	0.48
O_ISC_2	1.60	0.62	S_SEIS_5	1.95	0.51
O_ISC_3	1.90	0.53	S_SEIS_6	2.30	0.43
E_PEP_1	1.35	0.74	S_SEIS_7	2.26	0.44
E_PEP_2	1.35	0.74	S_SEIS_8	1.84	0.54
E_GP_1	1.19	0.84	TRU_1	1.30	0.77
E_GP_2	1.19	0.84	TRU_2	1.37	0.73
S_PP_1	1.07	0.93	TRU_3	1.62	0.62
S_PP_2	1.22	0.82	TRU_4	1.51	0.66
S_PP_3	1.24	0.80	INTENT_1	1.25	0.80
S_PS_1	1.24	0.81	INTENT_2	1.25	0.80
S_PS_2	1.26	0.79	INTENT_3	1.13	0.88

5.5.4 Independent Sample T-test

The dataset was split by selecting first half (112) and second half (112) samples, which were grouped by grouping code ‘1’ and ‘2’ for the independent sample t-test for non-response bias. Because the sample size was 225, one sample was not included in sub samples to make even equal numbers of independent samples. The sub-samples were analysed for two-sample independent t-test at 5% significance level. Table 5.7 presents the results of independent sample t-test. The results show no significant difference in mean for first and second wave of responses. Only higher mean difference observed was for items S_SEIS_4 and S_SEIS_6 with mean differences 1.0 and 1.027. This is however not regarded as highly significant difference in mean values between independent samples chosen for the test.

Table 5.7 Two (Independent) Sample T-test

Factors	T-value	P-value	Mean Differences	Standard Error Difference	Factors	T-value	P-value	Mean Differences	Standard Error Difference
T_PU_1	2.101	0.037	0.241	0.115	S_PS_3	2.489	0.014	0.205	0.083
T_PU_2	3.141	0.002	0.241	0.077	S_PS_4	5.116	0.000	0.482	0.094
T_PU_3	1.633	0.104	0.181	0.111	S_SEIS_1	3.339	0.001	0.304	0.091
T_FR_1	5.572	0.000	0.536	0.096	S_SEIS_2	8.272	0.000	0.830	0.100
T_FR_2	6.088	0.000	0.589	0.097	S_SEIS_3	9.020	0.000	0.884	0.098
O_ISC_1	5.197	0.000	0.491	0.094	S_SEIS_4	10.433	0.000	1.000	0.096
O_ISC_2	8.391	0.000	0.813	0.097	S_SEIS_5	7.638	0.000	0.750	0.098
O_ISC_3	7.331	0.000	0.661	0.090	S_SEIS_6	10.014	0.000	1.000	0.103
E_PEP_1	5.523	0.000	0.527	0.095	S_SEIS_7	7.308	0.000	0.821	0.112
E_PEP_2	3.122	0.002	0.268	0.086	S_SEIS_8	7.821	0.000	0.768	0.098
E_GP_1	4.232	0.000	0.411	0.097	TRU_1	2.198	0.029	0.161	0.073
E_GP_2	5.487	0.000	0.571	0.104	TRU_2	1.456	0.147	0.125	0.086
S_PP_1	3.022	0.003	0.223	0.074	TRU_3	6.104	0.000	0.670	0.110
S_PP_2	3.790	0.000	0.402	0.106	TRU_4	6.720	0.000	0.795	0.118
S_PP_3	3.601	0.000	0.286	0.079	INT_1	3.445	0.001	0.304	0.088
S_PS_1	4.188	0.000	0.366	0.087	INT_2	3.996	0.000	0.384	0.096
S_PS_2	1.597	0.112	0.205	0.129	INT_3	2.113	0.036	0.232	0.110

5.6 Instrument Validation and Measurement Model

In a scientific research, all the instruments must be validated by referring to the previously validated instruments wherever possible, for the sake of efficiency (Boudreau et al., 2001). Verification of instrument items with the help of correct measurement of the proposed model is an essential part of any scientific research (Paschke, 2009). However, there is always a possibility of measurement errors in scientific research. The measurement errors can be reduced to an acceptable level by adopting a proper research approach. Therefore, to minimise the measurement error, the research instruments need to be validated using a systematic approach.

5.6.1 Content Validity

When measurement scale is developed for a research study, the procedure followed should provide comprehensive information about the reliability and validity of the scale. Content validity is the extent to which research an instrument consists of an adequate sample of items for the measured construct (Hair et al., 2014). It is considered essential for determining quality of the scale used (Polit & Beck, 2006). The definition of the content validity represents the idea being a matter of judgement, careful conceptualisation and analysis of the scale prior to items generation. Literature review can be helpful in achieving content validity where previously validated and accepted instruments are followed in the research. This study conducted an extensive literature review on innovation and technology adoption models in the information systems discipline. Chapter 3 presents a review of existing technology adoption models and their suitability in various settings. Of these models, TOE stands out because of its support with studying factors associated with technology, organisation and environment in relation to the adoption of innovative technologies. While the adoption related factors can be studied with the TOE model, it does not consider security as the key determinant in influencing new technology adoption. As security is seen as critical in the adoption of new technologies such as smart cities, the security component has been considered. The proposed model consists of eight factors – namely functionality and reliability, perceived usefulness, information security culture, government policy, perceived external pressure, perceived privacy, perceived security and self-efficacy in information security - for determining the trust based smart city adoption intention. Also, Chapter 3 defines and justifies factors and their relationship with trust and intention to adopt the technology using existing technology adoption frameworks discussed in the literature. This ensures that instruments developed for this study have sufficient content validity.

5.6.2 Reliability Analysis

Reliability study is often used for the purification of the measurement instruments. Reliability analysis is the way of assessing errors within the constructs (Kimberlin & Winterstein, 2008). Reliability study of the research instruments can identify the items that do not belong to the expected same dimension and do not measure towards the same thing, which may produce another dimension in the factor analysis, and are to be deleted (Churchill, 1979). Straub, et al., (2004) indicate six different approaches to assess the reliability of the constructs such as split-half, test-retest, inter-rafter, unidimensional, alternative forms and internal consistency. Among all, internal consistency reliability analysis method is used for the reliability analysis of the constructs in this study. Churchill (1979) recommends item-to-total correlation (also known as item-scale) and Cronbach's alpha (alpha hereafter) as most widely used statistics to assess reliability for internal consistency. Churchill (1979) suggests that Cronbach's alpha should be the first calculation to measure the instrument's quality. Cronbach's alpha and item-scale were calculated using IBM SPSS version 26, for each construct separately. The literature does not agree upon a single threshold for the alpha values and the threshold is variable depending on the number of items per each construct, where a higher number of items in a construct yields a higher alpha (Churchill, 1979).

Another approach to measure internal reliability is by using Cronbach's alpha and AVE values (Lew & Sinkovics, 2012). George and Mallery (2003) suggest that Cronbach's alpha values above 0.7 are acceptable and the higher range is always considered highly reliable. Interestingly, researchers presented various arguments for a threshold. For example, Hair et al. (2014) point out that alpha values above 0.6 can be considered reliable and suggest checking the item reliability with other measures when the value falls below 0.5. However, Jöreskog and Sörbom (1984) recommend accepting alpha values above 0.5 for further analysis.

Table 5.8 presents AVE, CR and Cronbach's alpha values for the constructs presented in the research model. The alpha values for the items have been checked and the values presented in Table 5.8 suggest that AVE values are above 0.5. Hence, these items are accepted for further analysis.

Table 5.8 Reliability Scores of the Constructs

Dimensions	Construct	Items	Factor Loading	Sample Mean	Standard Deviation	t-statistics	CR*	AVE**
Technology	T_PU	T_PU_1	0.72	0.717	0.05	14.276	0.808	0.584
		T_PU_2	0.77	0.768	0.041	19.011		
		T_PU_3	0.80	0.797	0.034	23.579		
	T_FR	T_FR_1	0.89	0.888	0.025	35.667	0.891	0.804
		T_FR_2	0.90	0.904	0.018	49.182		
Organisation	O_SCA	O_SC_1	0.76	0.758	0.043	17.555	0.868	0.688
		O_ISC_2	0.84	0.844	0.022	39.083		
		O_ISC_3	0.88	0.879	0.017	52.553		
Environment	E_PEP	E_PEP_1	0.88	0.884	0.02	44.699	0.860	0.754
		E_PEP_2	0.85	0.849	0.032	26.995		
	E_GP	E_GP_1	0.80	0.792	0.062	12.785	0.822	0.699
		E_GP_2	0.87	0.872	0.038	22.677		
Security	S_PP	S_PP_1	0.50	0.484	0.106	4.643	0.758	0.522
		S_PP_2	0.78	0.768	0.054	14.437		
		S_PP_3	0.85	0.849	0.034	24.75		
	S_PS	S_PS_1	0.66	0.663	0.054	12.347	0.803	0.506
		S_PS_2	0.72	0.716	0.044	16.255		
		S_PS_3	0.75	0.752	0.038	19.924		
		S_PS_4	0.71	0.704	0.05	14.282		
	S_SEIS	S_SEIS_2	0.75	0.745	0.035	21.055	0.898	0.535
		S_SEIS_3	0.83	0.829	0.024	34.153		
		S_SEIS_4	0.77	0.773	0.024	31.896		
		S_SEIS_5	0.76	0.753	0.042	18.206		
		S_SEIS_6	0.80	0.802	0.028	28.92		
		S_SEIS_7	0.76	0.753	0.037	20.639		
		S_SEIS_8	0.74	0.734	0.033	22.365		
Trust	TRU	TRU_1	0.68	0.679	0.049	14.073	0.834	0.558
		TRU_2	0.72	0.698	0.046	15.4		
		TRU_3	0.80	0.826	0.02	40.708		
		TRU_4	0.77	0.77	0.029	26.544		
Adoption Intention	INT	INT_1	0.77	0.845	0.026	32.246	0.779	0.546
		INT_2	0.78	0.771	0.05	15.354		
		INT_3	0.68	0.564	0.084	6.758		

Note: CR – Composite Reliability, AVE – Average Variance Extracted

After assessing content validity, the next step to follow is to ensure construct validity. The upcoming sections will discuss the construct validity of the data using factor analysis approaches.

5.7 Structural Model Examination

To analyse the underlying structure between the items of a measurement model, an interdependence approach known as factor analysis is used (Lewis-Beck et al., 2004). Factor analysis is a set of tools to facilitate analysis of structural interrelationships or correlations among multiple variables by defining the group of highly interrelated variables (Hair et al., 2014). Factor analysis can help draw collective meaning for the set of conceptual predefined variables. There are two approaches of factor analysis, which are exploratory factor analysis (EFA) and confirmatory factor analysis (CFA). There is no single agreement for the specific role of each of these approaches but both approaches have their benefit to identify the interrelationship between variables. Most often, factor analysis is useful for minimising the number of items theorised, to a minimum number for the purpose of modelling (Hair et al., 2014).

5.7.1 Exploratory Factor Analysis

Exploratory factor analysis (EFA) is useful in the situation when relationships between the observed and latent variables are not obvious because of applying an existing research model in a different context (Byrne, 2013). Before attempting EFA, it is essential to ensure that a conceptual assumption is made, because even though EFA identifies the interrelationship between the items and variables, the relationships observed should be conceptually appropriate for factor analysis. Literature reviews in Chapters 3 and 4 have conceptualised a theoretical model with proposed relationships between variables.

To ensure that factor analysis is the appropriate approach for the data, the following tests were carried out. First, Bartlett's test of Sphericity (Lewis et al., 2005) was conducted for ensuring factor analysis is appropriate for the data. The results of Bartlett's test of Sphericity should be at below 0.05 significance level to ensure inter-item correlations is satisfactory. Second, Kaiser-Meyer-Olkin (KMO) test was conducted to assess adequacy of the sampling. The lower threshold value of KMO is 0.5, where higher value indicates adequacy. The KMO and Bartlett's test of Sphericity results are shown in Tables 5.9 and 5.10 respectively. The results show KMO values 0.5 or above, which is accepted, and high chi-square value (3503.4) is observed, both at significance level below 0.05.

Table 5.9 KMO Measure of Sampling Adequacy (for each factor)

Construct	No. of items	KMO Measure of Sampling Adequacy	Bartlett's test of Sphericity p-values	Observation
Perceived Usefulness (T_PU)	4	0.64	< 0.05	EFA supported
Functionality and reliability (T_FR)	2	0.500	<0.05	EFA supported
Information Security culture (O_ISC)	3	0.67	<0.05	EFA supported
Government Policy (E_GP)	2	0.50	<0.05	EFA supported
Pressure from external partners (E_PEP)	2	0.50	<0.05	EFA supported
Self-efficacy in Information security (S_SEIS)	8	0.87	<0.05	EFA supported
Perceived Privacy (S_PP)	3	0.58	<0.05	EFA supported
Perceived Security (S_PS)	4	0.72	<0.05	EFA supported
Trust (TRU)	4	0.71	<0.05	EFA supported
Intention to adopt (INT)	3	0.62	<0.05	EFA supported

Table 5.10 Kaiser-Meyer-Olkin Measure of Sampling Adequacy (KMOSA)

KMO Sampling Adequacy Measure		0.897
Bartlett's Test of Sphericity	Approximate Chi-Square Value	3503.4
	df	561
	p	0.00

Principal component analysis (PCA) was used as a method for factor extraction as it is the most commonly used method for factor extraction in information technology research. Another widely used method for factor extraction is common factor analysis; however, both factor extraction methods yield a similar outcome in empirical research (Hair et al., 2006). Factors having eigenvalues higher than 1.0 are regarded as significant. Also, among two factor rotations oblique and orthogonal, the orthogonal rotation Varimax is the most popular method when it comes to data reduction. Hair et al. (2014) suggest significant factor loading at 95% level of confidence interval is >0.4 for the sample size of 225. So, summarised from above discussion, the rules for factor extraction used are:

- Factor Extraction method: PCA with eigenvalue threshold >1 indicating significance
- Rotation: Orthogonal (Varimax)
- Items with cross loading difference significant to be dropped
- The item with individual factor loading below 0.4 was dropped

Table 5.11 shows the results of exploratory factor analysis (EFA).

Table 5.11 Exploratory Factor Analysis (EFA) Results

Domain	Constructs	Items	Factors									
			1	2	3	4	5	6	7	8	9	10
Technology	T_PU	T_PU_1	0.72									
		T_PU_2	0.77									
		T_PU_3	0.80									
	T_FR	T_FR_1		0.89								
		T_FR_2		0.90								
Organisation	O_SCA	O_ISC_1			0.76							
		O_ISC_2			0.84							
		O_ISC_3			0.88							
Environment	E_PEP	E_PEP_1				0.88						
		E_PEP_2				0.85						
	E_GP	E_GP_1					0.80					
		E_GP_2					0.87					
Security	S_PP	S_PRV_1						0.49				
		S_PRV_2						0.78				
		S_PRV_3						0.85				
	S_PS	S_SEC_1							0.66			
		S_SEC_2							0.72			
		S_SEC_3							0.75			
		S_SEC_4							0.71			
	S_SEIS	S_SEIS_1								0.33*		
		S_SEIS_2								0.75		
		S_SEIS_3								0.83		
		S_SEIS_4								0.77		
		S_SEIS_5								0.76		
		S_SEIS_6								0.80		
		S_SEIS_7								0.76		
		S_SEIS_8								0.74		
Trust	TRU	TRU_1									0.68	
		TRU_2									0.72	
		TRU_3									0.80	
		TRU_4									0.77	
Adoption Intention	INT	INT_1										0.77
		INT_2										0.78
		INT_3										0.68

Note: * = items with < 0.4 factor loadings

Hair et al. (2014) suggest factors as low as 0.4 can be accepted for the sample size above 200 at 95% level of confidence. The exploratory factor analysis shows one item S_SEIS_1 with 0.33 factor loading, which is less than the threshold of 0.4. The item S_SEIS_1 was deleted to maintain reliability of the construct. It is therefore suggested to use CFA than EFA when researcher has explored the literature to support the underlying factor structure of the model (Russell, 2002). However, EFA can conduct a preliminary analysis of the data to check whether data represents the proposed model. Some items were deleted because of having very low individual factor loading and very high cross factor loadings. Deleted item based on the observed factor loadings (Table 5.11) is presented in Table 5.12.

Table 5.12 Deleted Items after Preliminary Exploratory Factor Analysis

Item	Label	Factor Loading	Remarks
S_SEIS_1	I feel confident handling virus infected files	0.325	Item deleted because of loading less than 0.4

5.7.2 Coefficient of Determination (R^2)

The explanatory power of the structural model was assessed by using coefficient of determination (R^2) values as shown in Table 5.13, which represents the extent of variation in regression model from the baseline (0) (Hair et al., 2014). The t-values were used to assess statistical significance of each path coefficient. The threshold of R^2 values for endogenous constructs indicated by Chin (1998) are 0.67, 0.33 and 0.19 depicting substantial, moderate and weak. As indicated in Table 5.13, R^2 values for Trust is 0.582, which means 58.2% of variance in trust is explained by exogenous constructs. This means observed variance of trust can be interpreted as at upper range with respect to Chin's (1998) suggestion. Similarly, adoption intention, with the variance of 27.9% explained by the construct trust, has small variance.

Table 5.13 R^2 Values for the Endogenous Constructs

	R^2	Q^2	Standard Deviation	T Statistics	P-Values
INTENT	0.279	0.14	0.056	4.989	0.00
TRUST	0.582	0.293	0.046	12.739	0.00

5.7.3 Assessment of f^2

The values of f^2 and Q^2 are used to measure the quality criteria of the structural model (Peng & Lai, 2012). The influence of predictor variable on R^2 values of the endogenous variables is evaluated by using f^2 effect size (Peng & Lai, 2012). All relationships indicate small f^2 effect size except trust and intent to adopt relationship, which has large effect size with a value of 0.387. Table 5.14 shows the f^2 values for the paths in the structural model.

Table 5.14 f^2 Values for the Paths in the Structural Model

Constructs influence	f^2 values	Sample Mean (M)	Standard Deviation
E_GP -> TRUST	0.013	0.019	0.02
E_PEP -> TRUST	0.057	0.063	0.04
O_ISC -> TRUST	0.024	0.033	0.03
S_PP -> TRUST	0.018	0.025	0.02
S_PS -> TRUST	0.084	0.093	0.05
S_SEIS -> TRUST	0.004	0.011	0.01
TRUST -> INTENT	**0.387**	0.408	0.11
T_FR -> TRUST	0.00	0.007	0.01
T_PU -> TRUST	0.067	0.077	0.04

5.7.4 Assessment of Predictive Relevance (Q^2)

Another quality criterion of the structural model was assessed via Stone-Geisser's Q^2, which was conducted for predictive relevance using SmartPLS blindfolding technique (Hair et al.,

2014; Peng & Lai, 2009). The motive of the Q^2 measure is to determine to what degree the model's prediction is successful. According to Hair et al. (2014), the Q^2 value is only applicable to the endogenous variables, where positive value indicates predictive relevance. Therefore, Q^2 values are obtained only for trust and adoption intention in this study. Both endogenous constructs had Q^2 values above 0, as indicated in Table 5.15, which confirms the predictive relevance of endogenous constructs in the structural model.

Table 5.15 Q^2 Results for Endogenous Constructs

Constructs	SSO	SSE	$Q^2 = (1-SSE/SSO)$
INTENT	675	580.41	0.14
TRUST	900	636.321	0.293

5.7.5 Confirmatory Factor Analysis

After exploratory factor analysis, confirmatory factor analysis (CFA) was carried out. As SmartPLS allows the researcher to draw the structural model and test the validity of individual constructs, the SEM was used for establishing the model validity. A prior theoretical model of the constructs is required for the CFA, where loading of cross factors is pre-defined (Byrne, 2013). This means CFA only deals with the relationship between factors and their measurement variables. The generally used statistical criteria to assess the validity of the measurement model involves goodness of fit indices, convergent validity and discriminant validity. Table 5.16 presents factor loadings, sample mean, standard deviation, t-statistics, construct reliability and average variance extracted for all the constructs presented in the research model.

Table 5.16 Psychrometric Properties of the Constructs

Dimensions	Construct	Items	Factor Loading	Sample Mean	Standard Deviation	t-statistics	CR*	AVE**
Technology	T_PU	T_PU_1	0.72	0.717	0.05	14.276	0.808	0.584
		T_PU_2	0.77	0.768	0.041	19.011		
		T_PU_3	0.80	0.797	0.034	23.579		
	T_FR	T_FR_1	0.89	0.888	0.025	35.667	0.891	0.804
		T_FR_2	0.90	0.904	0.018	49.182		
Organisation	O_SCA	O_SC_1	0.76	0.758	0.043	17.555	0.868	0.688
		O_ISC_2	0.84	0.844	0.022	39.083		
		O_ISC_3	0.88	0.879	0.017	52.553		
Environment	E_PEP	E_PEP_1	0.88	0.884	0.02	44.699	0.860	0.754
		E_PEP_2	0.85	0.849	0.032	26.995		
	E_GP	E_GP_1	0.80	0.792	0.062	12.785	0.822	0.699
		E_GP_2	0.87	0.872	0.038	22.677		
Security	S_PP	S_PP_1	0.50	0.484	0.106	4.643	0.758	0.522
		S_PP_2	0.78	0.768	0.054	14.437		
		S_PP_3	0.85	0.849	0.034	24.75		
	S_PS	S_PS_1	0.66	0.663	0.054	12.347	0.803	0.506
		S_PS_2	0.72	0.716	0.044	16.255		
		S_PS_3	0.75	0.752	0.038	19.924		
		S_PS_4	0.71	0.704	0.05	14.282		
	S_SEIS	S_SEIS_2	0.75	0.745	0.035	21.055	0.898	0.535
		S_SEIS_3	0.83	0.829	0.024	34.153		
		S_SEIS_4	0.77	0.773	0.024	31.896		
		S_SEIS_5	0.76	0.753	0.042	18.206		
		S_SEIS_6	0.80	0.802	0.028	28.92		
		S_SEIS_7	0.76	0.753	0.037	20.639		
		S_SEIS_8	0.74	0.734	0.033	22.365		
Trust	TRU	TRU_1	0.68	0.679	0.049	14.073	0.834	0.558
		TRU_2	0.72	0.698	0.046	15.4		
		TRU_3	0.80	0.826	0.02	40.708		
		TRU_4	0.77	0.77	0.029	26.544		
Adoption Intention	INT	INT_1	0.77	0.845	0.026	32.246	0.779	0.546
		INT_2	0.78	0.771	0.05	15.354		
		INT_3	0.68	0.564	0.084	6.758		

Note: CR – Composite Reliability, AVE – Average Variance Extracted

5.7.6 Measurement Model

The measurement model developed for this study uses reflective as well as formative model. The indicator-to-independent variable relationships are reflective and relationships between dependent and independent variables are formative. The evaluation process of the measurement model followed the guidelines of Becker et al. (2012). There are no mediating effects or higher and lower level constructs designed in the model. The types and nature of various measurement models are discussed in Chapter 4. Figure 5.5 shows the reflective-formative measurement model used in this study.

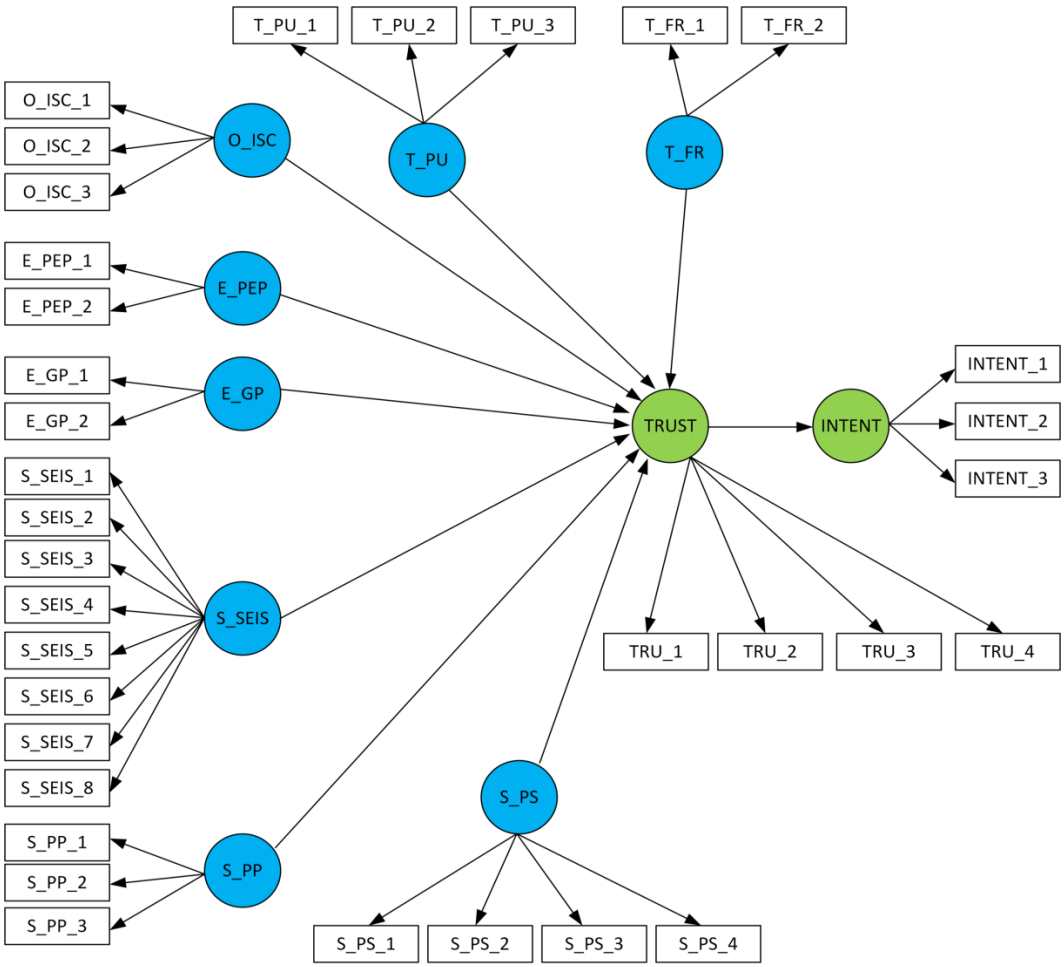


Figure 5.5 Measurement Model for the Research Framework

5.7.7 Indicator Validity, Convergent Validity and Discriminant Validity

Prior to hypothesis testing, indicators, constructs, convergent and discriminant validity were assessed. This section presents the statistical test results for each test conducted.

5.7.7.1 Indicator Validity

Indicator validity for relationship between independent factors and dependent factors was assessed with the help of magnitude, sign and significance of the path coefficient (Andreev et al., 2009). The threshold for path coefficient is 0.1 or above for it to be statistically significant and being consistent with the proposed model (Andreev et al., 2009).

Table 5.17 presents the summary of the test for indicator validity for all constructs. Bootstrapping procedure was used to estimate the significance of the path coefficients. The result suggests a total of five constructs have insignificant path coefficients, which are identified in bold. Only four paths met the t-value's required minimum threshold of 1.96 with p-values below 0.05. The result also indicates negative path coefficient for 'T_FR' to 'Trust' relationship, with the path coefficient near zero and t-value of 0.246. Since the model uses reflective-formative constructs, deletion of a construct in the formative model omits part of the constructs (Bollen & Lennox, 1991). Therefore, no constructs were omitted based on the test result for indicator validity.

Table 5.17 Results for Indicator Validity of the Reflective-Formative Constructs

Domain	Path	Path Coefficient (β)	T-value	P-Values
Technology	T_FR -> TRUST	-0.02	**0.246**	0.805
	T_PU -> TRUST	0.22	3.681	0.00
Organisation	O_ISC -> TRUST	0.16	**1.848**	0.065
Environment	E_GP -> TRUST	0.10	**1.546**	0.122
	E_PEP -> TRUST	0.20	3.162	0.002
Security	S_PP -> TRUST	0.12	**1.822**	0.068
	S_PS -> TRUST	0.25	3.817	0.00
	S_SEIS -> TRUST	0.05	**0.78**	0.436
	TRUST -> INTENT	0.53	9.805	0.00

5.7.7.2 Convergent Validity

Convergent validity is an assessment depicting whether items within a same variable measure the same thing by revealing correlation among them. Hair et al. (2014) indicate convergent validity in CFA as a measure of whether a proportion of variance is shared by items of the same latent factor. Convergent validity is achieved when factor loading is significantly different from zero (Bagozzi et al., 1991). Further, regression weights higher than 0.5 and Squared Multiple Correlations (SMC) greater than 0.7 can be optimal for the convergent validity (Hair et al., 2014). Similarly, Hair et al. (2014) suggest statistical criteria for achieving convergent validity is achieved by evaluating factor loading of indicators, composite reliability (CR) and average variance extracted (AVE). When CR value is higher than 0.7, internal consistency is regarded as satisfactory while values between 0.6 and 0.7 are considered acceptable but CR value below 0.6 indicates lack of reliability (Hair et al., 2010). Similarly, when AVE value of the construct is at least 0.5, sufficient convergent validity can be achieved, and it indicates at least 50% of the variance among the indicators (Fornell & Larcker, 1981; Henseler et al., 2015). Results in Table 5.16 show AVE values above the threshold of 0.5 for all constructs, where all values are within the range of 0.506 and 0.804.

This demonstrates enough convergent validity. Also, CR values represented in Table 5.16 shows it is higher than 0.758 for all factors. This indicates internal consistency is satisfactory for all factors.

5.7.7.3 Discriminant Validity

Discriminant validity measures to what extent latent constructs are differentiating from one another empirically (Hamid et al., 2017). It is a measure between the variables, which is useful in the situation when latent variables and constructs are interrelated. Correlation and average variance extracted (AVE) along with model fit statistics are generally used to measure discriminant validity (Holmes-Smith et al., 2006). Correlation above 0.9 indicates deficiency of discriminant validity and AVE value should be higher than square of correlations among the constructs (Holmes-Smith et al., 2006). Many researchers previously used Fornell and Larcker criterion to assess discriminant validity, which was proposed by Fornell and Larcker (1981). However, this approach was discouraged for assessing discriminant validity (Henseler et al., 2015), claiming that Fornell and Larcker criteria fail to establish distinction between the constructs. Thus, heterotrait-monotrait (HTMT) ratio of correlation method was introduced as superior performing method to assess discriminant validity.

HTMT values close to 1 signify lack of discriminant validity. Kline et. al. (2012) recommend threshold value for HTMT as 0.85, where Gold et al. (2001) and Henseler et al. (2015) indicate 0.9 as the threshold. The HTMT test results presented in Table 5.18 indicate that the values are within the acceptable threshold establishing discriminant validity. Hence, these values are considered for further analysis.

Table 5.18 Heterotrait - Monotrait (HTMT) Ratio of Correlations

	E_GP	E_PEP	INTENT	O_ISC	S_PP	S_PS	S_SEIS	TRUST	T_FR
E_PEP	0.35								
INTENT	0.35	0.55							
O_ISC	0.88	0.64	0.61						
S_PP	0.48	0.49	0.9	0.43					
S_PS	0.47	0.53	0.74	0.65	0.75				
S_SEIS	0.73	0.51	0.52	0.78	0.51	0.67			
TRUST	0.58	0.81	0.74	0.74	0.68	0.81	0.62		
T_FR	0.4	0.52	0.77	0.61	0.83	0.74	0.56	0.62	
T_PU	0.31	0.89	0.84	0.53	0.68	0.54	0.38	0.80	0.65

5.8 Summary of the Hypothesis Test

Table 5.19 presents the results of the hypothesis test. The hypothesis test results will be discussed in Chapter 6, where each hypothesis will be discussed by comparing and analysing the results with prior research results. The test results in Table 5.19 shows only four hypotheses were supported, which will be discussed in the next chapter.

Table 5.19 Hypothesis Test Summary

Hypotheses	β	t-statistics	P value	Remarks
H1: Functionality and reliability positively influences stakeholders trust in smart city services and technologies.	-0.020	0.292	0.77	Rejected
H2: Perceived usefulness positively influences stakeholders' trust in smart city services and technologies.	0.224	3.65	0.000	Supported
H3: Stakeholders' information security culture positively influences their trust in smart city services and technologies.	0.16	1.8	0.072	Rejected
H4: Perceived external pressure positively influences stakeholders' trust on smart city services and technologies.	0.20	2.99	0.003	Supported
H5: Government policy positively influences towards stakeholders' trust on smart city services and technologies.	0.093	1.5	0.134	Rejected
H6: Perceived privacy positively influences stakeholders' trust in smart city services and technologies.	0.117	1.8	0.07	Rejected
H7: Perceived information security positively influences stakeholders' trust in smart city services and technologies.	0.25	3.88	0.000	Supported
H8: Self-efficacy in information security positively influences stakeholders' trust in smart city services and technologies.	0.529	0.72	0.47	Rejected
H9: Trust in smart city services and technologies positively influences stakeholders' intention to adopt smart city services and technologies.	0.528	9.69	0.000	Supported

5.9 Conclusion

The purpose of this chapter is to present the methods used for preparation and cleaning of data, which followed the approaches such as normality test, outlier identification, multicollinearity test, t-test, content validity, reliability analysis, confirmatory factor analysis, convergent validity and discriminant validity. The EFA results were discussed to indicate the trustworthiness of the measurement instrument. The results from Chapter 5 will be used to discuss the hypothesis test results in the following chapter.

6 Findings and Discussion

6.1 Introduction

Since the proposed research model had eight hypotheses in four categories - Technology, Organisation, Environment and Security - discussion of the results will be oriented to those categories. Findings of the data analysis are discussed in light of existing literature, and consistency or otherwise of the prior study's findings are reported. Section 6.2 discusses the results of each hypothesis test by comparing and contrasting the results with prior study outcomes. Section 6.3 discusses how each of the research questions is addressed by the research results. Section 6.4 concludes the chapter. The organisation of the Chapter 6 is shown in Figure 6.1.

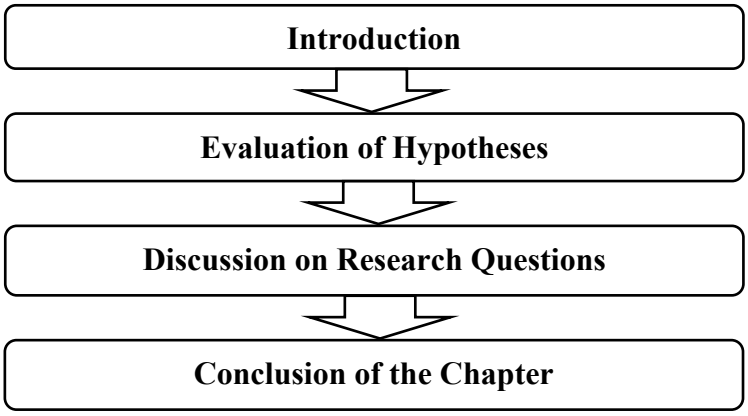


Figure 6.1 Overview of Chapter 6

6.2 Evaluation of Hypotheses

Table 6.1 presents the summarised test results of standardised path coefficient, t-statistics and significance levels to make remarks on whether to support the hypotheses. The results clearly show four hypotheses have been supported. To test the significance of the path of measurement model, bootstrapping method was used in PLS-SEM. Bootstrap is an alternative

and recommended way of producing better approximation, usually if the sample is small (Schmidheiny, 2012). Hair et al. (2011) recommend a minimum number of sub-samples for bootstrap as 5000 and it was the method used for obtaining test results in this study. For the purpose of hypothesis testing, the critical t-values for two-tailed test are regarded as 1.65, 1.96 and 2.58 for 10%, 5% and 1% level of significance respectively (Hair et al., 2014). Also, for multicollinearity, variance inflation factor (VIF) values of each items should be less than 5 as indicated by Hair et al. (2011). Each hypothesis will be discussed in the next section.

Table 6.1 Results for the Hypothesised Relationships

Hypothesis	β	t-value	P value	Remarks
H1: Functionality and reliability positively influences stakeholders' trust in smart city services and technologies.	-0.020	0.292	0.77	Rejected
H2: Perceived usefulness positively influences stakeholders' trust in smart city services and technologies.	0.224	3.65	0.000	Supported
H3: Stakeholders' information security culture positively influences their trust in smart city services and technologies.	0.16	1.8	0.072	Rejected
H4: Perceived external pressure positively influences stakeholders' trust on smart city services and technologies.	0.20	2.99	0.003	Supported
H5: Government policy positively influences towards stakeholders' trust on smart city services and technologies.	0.093	1.5	0.134	Rejected
H6: Perceived privacy positively influences stakeholders' trust in smart city services and technologies.	0.117	1.8	0.07	Rejected
H7: Perceived information security positively influences stakeholders' trust in smart city services and technologies.	0.25	3.88	0.000	Supported
H8: Self-efficacy in information security positively influences stakeholders' trust in smart city services and technologies.	0.529	0.72	0.47	Rejected
H9: Trust in smart city services and technologies positively influences stakeholders' intention to adopt smart city services and technologies.	0.528	9.69	0.000	Supported

6.2.1 Technology Dimension

A total of two hypotheses (H1 and H2) were proposed for the technology dimension that relate perceived usefulness of the smart city services and functionality and reliability with trust. Path coefficient (β), T-values (t-value) and level of significance (p) were taken into account to make the decision on whether the hypotheses are supported or rejected. Table 6.1 shows the results of the hypothesis test.

6.2.1.1 Influence of Functionality and Reliability on Trust

Hypothesis 1: Functionality and reliability positively influence stakeholders' trust in smart city services and technologies.

The hypothesis H1 was proposed to relate functionality and reliability of smart city services and stakeholders' trust towards it. The results of hypothesis testing indicate β = -0.02, t-value = 0.292 and p-value higher than 0.05. The path coefficient is insignificant along with low t-value (below 1.96) and p-value is 0.77. These values suggest there is no significant impact of functionality and reliability towards stakeholders' trust on smart city services and technologies. In fact, there is a slight negative influence observed with negative path coefficient value, but the observed β value is close to zero and the result is not significant as p-value is significantly higher than 0.05. Hence, the hypothesis (H1) 'Functionality and reliability positively influence stakeholders' trust in smart city services and technologies' is (or has been) rejected.

This result contradicts the finding of AlHogail (2018), which found functionality and reliability as a positively influencing factor towards building trust. More importantly, the study of AlHogail was related to the adoption of Internet of Things (IoT) technology, which

is also a major enabling technology used in smart cities. Another study by McKnight et al. (2011) found a significant positive relationship between functionality and reliability with trust in technology. However, the study of McKnight et al. (2011) was conducted with the data collected by students and the technology evaluated for adoption study was use of computer software. Smart city services pose a unique characteristic and is a fairly new and innovative feature. As smart city technologies are still being rolled out, there are limited studies on the influence of functionality and reliability on trust. However, this study made use of existing knowledge to investigate the relationship between the two constructs. The results will lay a solid foundation for future studies aimed at investigating the role of functionality and reliability on trust. The final remark on the finding is that functionality and reliability of smart city services does not have significant positive influence on building trust in smart city services and technologies.

6.2.1.2 Influence of Perceived Usefulness on Trust

H2: Perceived usefulness positively influences stakeholders' trust in smart city services and technologies

The hypothesis was developed relating to perceived usefulness of the smart city services and technology, with stakeholders' trust. The results in Table 6.1 indicate β value of 0.224, t-value 3.65 and p-value below 0.05. The significant hypothesis test result suggests increased usefulness of smart city services and technologies may have significant positive influence towards increasing stakeholders' trust.

The findings are in line with the recent study of Zhang et al. (2019), where authors hypothesised perceived usefulness influences trust and found the significant path coefficient

(β) = 0.6 at p-value 0.001. However, this research was conducted to study the role of trust and perceived risk on user acceptance of automated vehicles. Similarly, the relationship between trust and perceived usefulness has been found significant by the study of Mou et al. (2017), where authors have studied the influence of trust and perceived usefulness related factors in consumer acceptance of e-services. Another study by Roca et al. (2009) also supported the result of the current study where the authors found an influencing relationship of perceived usefulness with users' trust related to online trading systems. Smart city services comprise several innovative ICT related services; thus, the results are compared with the previous studies on ICT related services, which used the same factors in the study. Thus, the validated outcome suggests stakeholders' perception on usefulness of smart city services increases the adoption of smart city services and technologies by stakeholders in regional Australian cities.

6.2.2 Organisation Dimension

The organisation dimension had only one factor: information security culture, hence only one hypothesis (H3) was proposed.

6.2.2.1 Influence of Information Security Culture on Trust

H3: Stakeholders' information security culture positively influences stakeholders' trust in smart city services and technologies.

Hypothesis 'H3' was developed to relate information security culture with trust on smart city services and technologies. This was the only hypothesis related to the organisation dimension. The results in Table 6.1 shows little significance of the path coefficient and significance level with β = 0.16 and t-value = 1.8, however because of p-value not being lower than 0.05 and t-value being lower than the threshold of 1.96, the hypothesis was

rejected. This means the influence of information security culture has not been found as significant towards building trust on smart city services and technologies.

Schlienger and Teufel (2003) theorise that trust can be increased by having appropriate information security culture. This is opposite to what the current research result shows. However, the proposition of Schlienger and Teufel (2003) has not been strongly supported by the empirical results. Although a higher level of information security compliance as a result of having effective information security culture has been found by AlKalbani et al. (2015), there is a lack of empirical evidence to understand whether information security culture has a positive or negative influence on adoption of smart city services. The result of the current study means further research is required to assess how information security culture influences stakeholders' trust towards their intention to adopt smart city services and technologies.

6.2.3 Environment Dimension

The environment dimension in this study consists of two factors: perceived external pressure and government policy.

6.2.3.1 Influence of Perceived External Pressure on trust

H4: Perceived external pressure positively influences stakeholders' trust on smart city services and technologies.

The test results presented in Table 6.1 show a positive path coefficient value at a level of significance below 0.05. The observed results show $\beta = 0.2$, t-value = 2.99 and p-value = 0.003. The significant result suggests hypothesis H4 is supported. This means external pressure positively influences stakeholders' trust on smart city services and technologies.

However, the low value of path coefficient indicates the influence of perceived external pressure on stakeholders' trust is less significant.

The result of hypothesis H4 is in accordance with the result of Duan et al. (2012), where researchers found significant direct influence of external pressure on perceived trust for the adoption of innovative technology such as e-Market. The study of e-Market adoption found $\beta = 0.44$ at p-value < 0.01. In contrast, a study by Plum and Stetter (2009) agrees that trust is negatively influenced if the negative pressure is applied in the organisation environment. However, the authors suggest trust is less impacted if the pressure is from external sources. This is in line with the finding of the current study. Distinguishing between different types of external pressure is important to categorise, to understand how different sources of pressure influence on trust. Smart city services being not limited to within a single organisation, pressure from internal and external sources can be challenging to distinguish. Finally, the low β value of the relationship between perceived external pressure and trust indicate that more study is needed to further validate the weak relationship found between the factors.

6.2.3.2 Influence of Government Policy on Trust

H5: Government policy positively influences towards trust on smart city services and technologies.

The positive influence of government policy towards trust was hypothesised in this study. The hypothesis H5 was rejected as the test results presented in Table 6.1 show $\beta = 0.093$, t-value = 1.5 and p-value 0.134, which is above the threshold of 0.05. While the beta value is positive, the results are not conclusive because of poor t-value and the p-value being insignificant. As per the values obtained, the government policies have no significant influence over stakeholders' trust on smart city services and technologies. However, the

positive β value paves the way for future research. Future studies in a similar setting may provide further details about the influence of government policies on stakeholders' trust. This suggests government policy does not have positive influence towards stakeholders' trust on smart city services and technologies.

Moreover, the result of a study by van Dongen et al. (2013) does not support the result of hypothesis H5, where authors have focused their study in relation to trust in government policy. Van Dongen et al.'s (2013) study was related to trusting the government decision to build the electronic infrastructure that may harm people in the long term. Knack and Zak (2003) also have different views on the relationship between government policy and trust, where the authors found significant positive impact of some government policies such as public policy on citizens' trust. However, study of Knack and Zak (2001) concluded only few public policies by government have impact on trust on the services, which do not include trust over adoption of innovative technologies like smart city services. The study results may differ when it comes to developing a service that does not have direct negative impact upon the citizens and stakeholders. Government policy significantly determines to what extent stakeholders and users are benefited by smart city and what level of control and security features are applied on the smart services. The study outcome shows stakeholders are not convinced that government policy influences their level of trust on smart services. There certainly are more factors than government policy to influence trust in smart city services and technologies.

6.2.4 Security Dimension

There were three hypotheses within the security dimensions which relate perceived privacy, perceived information security and self-efficacy of information security with trust.

6.2.4.1 Influence of Perceived Privacy on Trust

H6: Perceived privacy positively influences stakeholders' trust in smart city services and technologies.

Hypothesis H6 was proposed to relate perceived privacy with trust in smart city services and technologies. The hypothesis test results yield path coefficient (β) = 0.117, t-value=1.8 at significance (p-value) = 0.07, which is below the required threshold of 0.05. This suggests the hypothesis is rejected, depicting no positive influence of perceived privacy on stakeholders' trust on smart city services.

The non-significant positive impact of perceived privacy on trust found by this study is supported by the study of Kassim (2017), where the researcher attempted to test the influence of perceived privacy and perceived security on trust. Kassim (2017) found that perceived privacy has very less significant impact on trust with the path coefficient (β) = 0.005 at p-value greater than 0.05. The study was, however, on user acceptance of internet banking. Conversely, the result of hypothesis H6 is not in line with the studies such as Liu et al. (2005) and AlHogail (2018), where the researchers found a positive influence of perceived privacy on trust. These studies were conducted on the subject of e-commerce and IoT technology adoption. However, the contradictory result of this research can be justified on the basis of its empirical nature as there are insufficient studies on trust-based adoption of smart cities. Shephard (2019) indicates there is something beyond privacy playing an influencing role to gain trust in smart city services. This means users and stakeholders are more concerned about other factors than privacy to trust the smart city services and technologies. Shephard (2019) claims that beyond the factors such as privacy, providing cost-effective services that yield real outcomes is needed to build strong trust in smart cities. Users' emphasis on a factor other

than privacy to trust smart cities might be the reason for the insignificant impact of privacy on trust found in this study.

6.2.4.2 Influence of Perceived Information Security on Trust

H7: Perceived information security positively influences stakeholders' trust in smart city services and technologies.

The hypothesis H7 was proposed to relate perceived information security and stakeholders' trust on smart city services and technologies. The results of the hypothesis test indicate β = 0.25, t-value = 3.88 and p-value below 0.05. These values suggest there is significant impact of perceived information security towards stakeholders' trust. Hence, the hypothesis H7 is supported on the basis of test results presented in Table 6.1.

The result of hypothesis H7 is in conjunction with the results of a number of prior studies such as Flavián and Guinalíu (2006), AlHogail (2018) and Kassim (2017). Flavián and Guinalíu (2006) found a significant positive influence of perceived security towards trust of internet consumers, which is also supported by this study. Prior studies related to trust on any ICT services have been regarded as comparable to the trust on ICT led smart city services. Security factor has a positive influence on users' trust when it comes to IoT technologies, which is also an enabling technology for smart cities (AlHogail, 2018). A research study by Kassim (2017) also found significant positive influence of perceived security on users' trust using internet-based services. The positive relationship between security and trust has been proven by this study when it comes to trusting ICT enabled smart city services.

6.2.4.3 Influence of Information Security Self-efficacy on Trust

H8: Self-efficacy in information security positively influences stakeholders' trust in smart city services and technologies.

Hypothesis H8 relates stakeholders' self-efficacy in information security and trust. The test results presented in Table 6.1 show a positive path coefficient value of β = 0.529. However, the t-value is 0.72, which is well below the required threshold of 1.96 and p-value is significantly higher than 0.05. This means the hypothesis is rejected, depicting self-efficacy in information security as not having a positive influence towards stakeholders' trust on smart city services and technologies.

There is a positive relationship found between trust and self-efficacy related to safe and proper use of internet-based services (Kim et al., 2009), which is not in line with the finding of this study. Information security self-efficacy has been linked with individuals' intention to adhere with the security compliance (Siponen et al., 2014). Prior research has found a significant positive impact of information security self-efficacy of an individual on their intention to strengthen security effort (Rhee et al., 2009). However, there are a limited number of studies to support the positive influence of information security self-efficacy on individuals' trust in technology, let alone the trust in smart city services. The result from this study suggested that there is no significant positive influence of information security self-efficacy on stakeholders' trust in smart city services and technology. This can be a valuable result for future studies.

6.2.5 Influence of Perceived Trust on Intention to Adopt

H9: Trust in smart city services and technologies positively influences stakeholders' intention to adopt smart city services and technologies.

To relate trust and stakeholders' intention to adopt smart city services and technologies, hypothesis H9 was proposed. The test result shown in Table 6.1 indicates β = 0.528, t-value

9.69 and p-value below the threshold level of 0.05. This indicates the relationship is significant and the hypothesis is supported. The result indicates stakeholders' trust on smart city services and technologies positively influences their intention to adopt. Both trust and intention to adopt being endogenous constructs show positive predictive relevance (Q^2) values of 0.14 and 0.29 respectively as shown in Table 5.15 in Chapter 5. The positive predictive relevance further supports the predicted positive influence of trust on intention to adopt.

The factors on trust and adoption have been previously examined by a number of studies related to technology adoption (Duan et al., 2012; Pavlou & Gefen, 2003). The result from this study is consistent with the prior research on technology adoption by Duan et al. (2012), where the authors have found a significant influence of perceived trust on the adoption of innovative e-commerce platform called e-Market. The authors, however, considered trust as a combination of trustworthiness of actual system as well as trustworthiness of external parties associated. Further, the outcome of the current study is also in line with the study of Pavlou and Gefen (2004), which strongly supports that trustworthiness of the smart technologies and services used in smart cities promotes adoption by the stakeholders. As concluded by Duan et al. (2012), the trustworthiness can also be associated with the external factors associated with the innovative technology and services used in smart cities. In support of the outcome of this study, Almuraqab and Jasimuddin (2017) have also theorised that trust in technology positively influences end users' intention to use smart-government services. The result of this study, as well as similar results from other related studies, suggest that in order to maximise the adoption of smart city services and technologies, trustworthiness of the individual services needs to be ensured. Althunibat et al. (2011) argue that people need to trust in government as well to ensure the new technology implemented by government is not for

monitoring and policing the users. Liu et al. (2005) also found a strong positive influence of trust towards consumers' adoption of an electronic service. Increasing trustworthiness of the services and technologies used in smart cities is an important factor to increase adoption of smart city services and technologies by its stakeholders.

6.3 Discussion on Research Questions

Chapter 1 presents three research questions that were framed from research problems, gaps, rationale and literature review. The research questioned framed were: What are the security challenges for smart cities? What are the determining factors on stakeholders' trust towards their intention to adopt smart city services and technologies in regional Australian cities? What are the recommendations for improving stakeholders' trust towards smart city adoption in regional Australian cities?

To address and investigate the research questions, a technology adoption model TOE, which is based on three broad dimensions - Technology, Organisation and Environment - was adopted. Based on the TOE model initially proposed by Tornatzky & Fleischer (1990), a new research model was developed in Chapter 3 by extending existing dimensions of TOE model to include security dimension. Chapter 2 conceptualises the smart city by discussing dimensions, entities, models and security challenges associated with smart cities. Smart city being a relatively new and broad concept, there is a question about whether the subject 'smart city' should be regarded as set of innovative technologies and system applied in the urban environment. Therefore, studies conducted on adoption of innovative technologies have been applied to frame the research model and to design the survey instrument. Some earlier researches such as Salleh and Janczewski (2016) presented TOE variables in relation to security to term their adoption model as Sec-TOE. However, because of significance

influence of trust towards technology adoption, the trust is presented as an endogenous variable which influences towards intention adoption of the smart city services and technology. The hypotheses are framed to identify the influence of factors in technology, organisation, environment and security dimensions towards stakeholders' trust and further influence of perceived trust towards their intention to adopt the smart city services. The complete research model and related hypotheses are presented in figure 6.2.

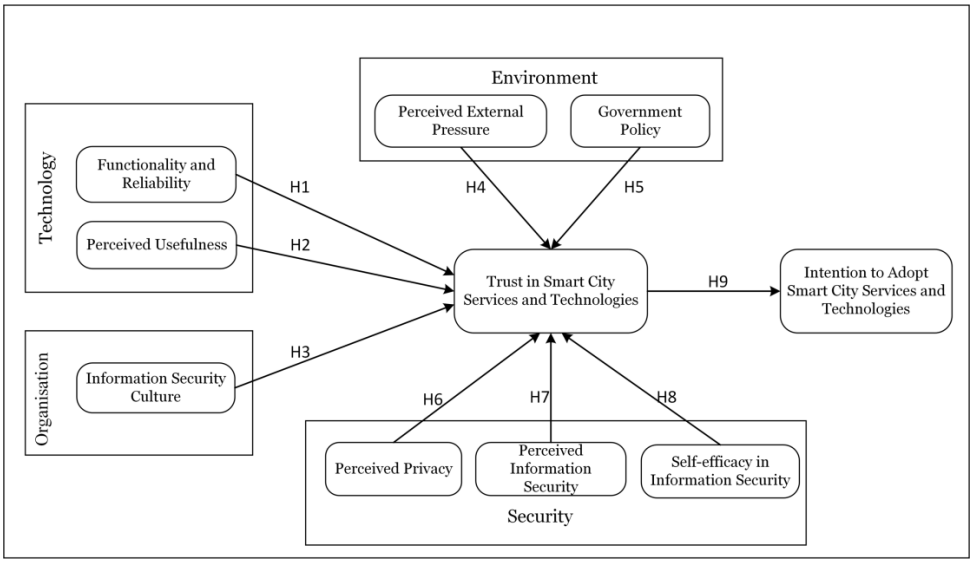


Figure 6.2 Research Model Revisited

6.3.1 What are the security challenges for smart cities?

Ijaz et al. (2016) presented information security factors derived from governance, technological and socio-economic factors. Literature review in Chapter 2 indicates smart city's security challenges mainly associated with the particular smart service or technology used such as smart grid system, building automation systems, unmanned aerial vehicles, smart vehicles, IoT sensors and cloud computing system (Baig et al. 2017). However, review of literature during the research model development resulted in three main security related factors influencing trust in smart city services. Based on the rigorous review of literature,

perceived privacy, perceived information security and self-efficacy in information security were identified as the top security related challenges, which influence towards building stakeholders' trust towards their intent to adopt smart city services. The hypothesis test result in table 6.1 shows only perceived information security has significant positive influence while perceived privacy has positive but less significant influence towards trust. In addition to security and privacy challenges, other challenges for smart city projects have been indicated as network connectivity, complexity of the networked infrastructure, security services and organisation of sensitive data Bartoli et al. (2011).

6.3.2 What are the determining factors on stakeholders' trust towards their intention to adopt smart city services and technologies in regional Australian cities?

Trust has been regarded as an important factor towards adoption of innovative technologies. Trust has also been used as a sub-domain of security when it is used in technology adoption studies. A number of factors were found to be used in study of technology adoption as presented in Chapter 3. The technology trust factor has been used along with the other variables such as perceived privacy, organisational culture and information security. Also, the security related factors such as perceived privacy and information security has been found influencing towards trust by AlHogail (2018) and Yeh (2017). Hence the second research question was formed to identify determinants of trust towards stakeholders' intention to adopt the smart services and technologies.

For addressing this research question, security related inputs (perceived privacy, perceived information security, self-efficacy in information security and organisation security culture) as well as non-security related inputs (functionality and reliability, perceived usefulness, pressure from external partners and government policy) were theorised and hypothesised.

Initially, the trust was formulated to be determined by eight variables within the dimensions of TOE and security as presented in figure 6.2. However, hypothesis test results showed perceived usefulness, perceived external pressure and perceived information security have significant positive influence towards trust. Moreover, two other variables, information security culture and perceived privacy have positive, but not significant, influence towards trust. Therefore, perceived usefulness, perceived external pressure and perceived information security can be regarded as highly influencing while information security culture in organisation and perceived privacy can be regarded as having less significant influence towards stakeholders' trust.

Finally, results indicate trust has significant positive relationship with intention to adopt. A significant and positive relationship between trust and intention to adopt indicates building up stakeholders' trust towards smart services and technologies integrated in smart city is key to successful adoption of smart city services and technologies.

6.3.3 What are the recommendations for improving stakeholders' trust towards smart city adoption in regional Australian cities?

Research question three was framed to provide recommendation for improving stakeholders' trust towards smart city adoption in regional Australian cities. The respondents' in the survey were from regional cities in Queensland, which suggests the research outcome can be regarded as most applicable in regional cities. The outcome of the data analysis indicates three most significant factors influencing towards stakeholders' trust are perceived usefulness, perceived external pressure and perceived information security. Based on the research outcome, three recommendations are provided to improve stakeholders' trust towards their intention to adopt smart city services in regional Australian cities. First,

assessment of usefulness of smart services and technologies being deployed is necessary for identifying on whether stakeholders regard individual smart services or technology is useful in the region. A widescale consultation technique such as crowdsourcing, should be used to generate perception of stakeholders to understand their view regarding usefulness of the individual smart city service or technology. The outcome of the widescale consultation with stakeholders can help understand the smart services or technologies that are perceived as useful in their region or cities.

The next recommendation is towards ensuring information security mechanisms of smart technologies are deployed. It is evident from the review of literature in Chapter 2 that security is one of the major issues in smart city infrastructure. This fact is also supported by the research outcome as a positive relationship is found between perceived information security and trust. The focus should be on mechanisms to ensure security of smart services and technologies, which will help building trust towards that smart services and technology projects being deployed. Since many Australian regional cities are considering implementing smart city projects, it is an appropriate time to include the aspect of information security from the planning or design phase of a project development. For this, appropriate information security personnel should also be involved in the project team. This can meet the concept of 'security by design' concept in the context of smart city projects deployment. Ensuring information security will help towards increasing stakeholders' trust so that they intend to accept and adopt smart services.

Finally, perceived privacy and information security culture in organisations is found to have a low positive influence towards stakeholders' trust. These are factors which need some attention to ensure security culture in organisation and privacy ensuring mechanism in the

smart city infrastructure. It is important to note that the involvement of information security personnel can ensure the successful implementation and use of smart city services or technologies. To preserve privacy, the data being generated and stored in the smart city environment should be categorised based on its sensitivity and handled accordingly. The access and transmission of data needs to be secured. Having information security consultants in smart city strategic teams is recommended, which may ensure stakeholders are not concerned about privacy issues so they can trust smart city services and technologies. Also, council and government websites and employee portals should provide enough information related to aspects of secure and privacy aware practice while working in digital environment. The organisational information security culture of an organisation should be managed by the organisation itself, with the help of training, awareness and policies for proper use of information technology within the organisation.

6.4 Conclusion

The chapter has assessed the hypotheses proposed in Chapter 3 to test how the proposed model is supported by the data. The data analysis results presented in Chapter 6 were used to discuss the outcomes by comparing and contrasting the results with the outcome of the prior studies. The positive influence of perceived trust towards stakeholders' intention to adopt smart city services has been found in the study. There were three factors, namely perceived usefulness, external pressure and perceived information security, that positively influence stakeholder trust. However, factors such as functionality and reliability, perceived privacy, government policy and self-efficacy in information security were not observed as having a positive influence towards trust. The comparisons of each of the hypothesis test results in this chapter have been made to understand how the current results stand with previous outcomes.

7 Conclusions

7.1 Introduction

This chapter provides the conclusion of this research by summarising theoretical and managerial implications of the study, limitations of the study and opportunities for future research. Section 7.2 of this chapter provides a summary of the current research study. Section 7.3 discusses the implications of this study, where theoretical and practical implications are discussed. Further, limitations of the research study and suggestions for future research are discussed in Section 7.4 and Section 7.5 respectively. Final remarks are made in Section 7.6. Figure 7.1 presents the structure of this chapter.

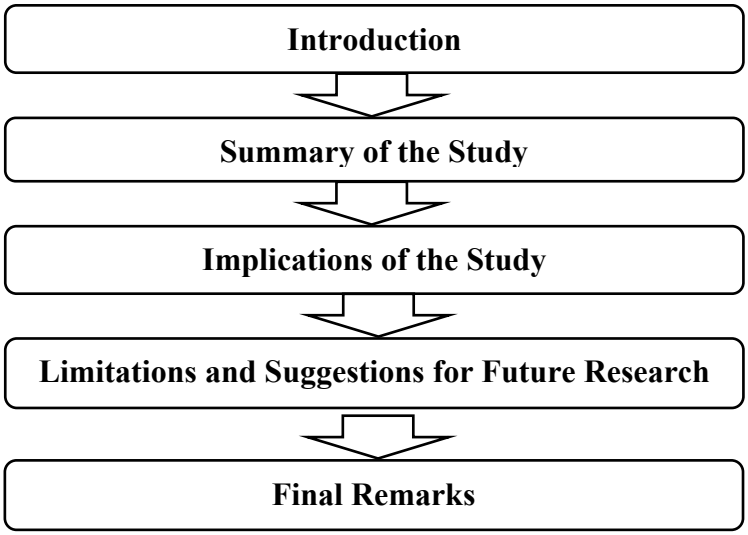


Figure 7.1 Overview of Chapter 7

7.2 Summary of the Study

Being an important factor towards technology adoption, trust has been acknowledged as a crucial determinant for adoption of innovative technology such as IoT (AlHogail, 2018). Adoption of smart city comprises adoption of its enabling technologies. Therefore, it is

important to consider adoption studies of innovative technologies such as IoT and Cloud computing while drawing conclusions from this study. Consideration of trust related factors is essential in order to improve stakeholders' trust towards adoption of smart city services and technologies. Smart city is indeed an advanced infrastructure, where technological, socio-economical, environmental, and organisational entities work together to facilitate an interconnected city framework. From a theoretical perspective, the complexity in relationships between trust related factors is evident. This study initially proposed a theoretical model using trust-based factors for stakeholder intention to adopt smart city services.

The factors were categorised using a well-known TOE model by extending the dimensions to introduce security domain. Security and trust have been correlated (AlHogail, 2018) and there is a positive influence of trust towards adoption intention Ratten (2014). The factors from TOE model and security determinants of trust, theorised from previous studies, have been evaluated using data from survey using questionnaire, where data was collected from ICT professionals working in regional Queensland. The stakeholders' view towards various security related questions was used to test and validate the proposed theoretical model. The SEM technique used for data analysis has provided several statistical significances to justify relationships between the observable and latent variables.

A total of nine hypotheses were developed from literature review to support the structural model. The results of the hypothesis testing revealed only four hypotheses were found significant and supported, while other results were contradictory with the findings of previous studies. However, the context of the study is unique because there are no prior studies on trust based smart city adoption. The results of this study are very important to understand

what factors play a part on trust and how trust influences adoption of smart city services and technologies.

7.3 Implications of the Study

This study has contributed to knowledge on information technology, smart city adoption, trust-based technology adoption and smart city security in a number of ways. The implications of the research results can be categorised theoretical and managerial.

7.3.1 Theoretical Implication

Firstly, this study hypothesised eight relationships to find factors' influence on stakeholders' trust on smart city services. The results found only three of the factors have significant influence on trust. That means three factors - perceived usefulness, external pressure and perceived security - contribute most towards building stakeholders' trust in smart city services, while other factors are less significant. This is an important finding in order to improve the stakeholders' trust towards their intention to adopt smart city services. Next, the research result significantly supported the positive influence of trust towards the intention to adopt smart city services and technologies by stakeholders. These results can be significant for academia as well as parties involved in development and implementation of smart cities.

Secondly, several technology adoption models and smart city initiative models have been analysed to support the proposed research model of this study. Accordingly, it was important to look at information security related factors as authors such as Ijaz et al. (2016), Baig et al. (2017), Gharaibeh et al. (2017) and Zhang et al. (2017) indicate that several security issues exist in smart cities. A study by Dewi et al. (2018) has incorporated the TOE model to assess smart city adoption decisions by using a theorised smart city readiness model. This study

adopted the TOE model to include security related dimensions for the intention to adopt innovative technologies and services. Bridging the theoretical gap associated with smart city technology adoption, based on stakeholders' trust, especially in the regional cities of Australia, was not explored yet.

Thus, security dimension was introduced in the research model and a new trust based smart city adoption framework called Technology, Organisation, Environment and Security (TOES) has been theorised.

7.3.2 Practical Implication

The practical implications of the result of this research study will be towards increased adoption and acceptance of smart city services by its stakeholders. City managers and planners can consider adopting the results of this study to gain support from stakeholders towards acceptance of innovative smart city services in their region. The result of this research study can support local government by informing them about how stakeholders' trust on smart city services and technologies can be built to increase adoption intention. The significant influence of trust on adoption intention observed by this study can help smart city policy makers to regard trust building mechanisms as an important subject for future adoption of smart city services and technologies by its stakeholders. For instance, perceived information security has been found as a significant factor towards building trust; hence, there should be sufficient security mechanism in the smart city to build stakeholders' trust and to increase smart city adoption.

Finally, the statistical significance of the validation process of the theorised model has provided a few significant findings that may help parties who are responsible for smart city

initiative and play a strategic role towards securing cities when they are equipped with the 'smart' features. Knowing trust enhancing factors that are validated by this study may help them to further explore the influencing factors for adoption of smart cities by various stakeholders.

7.4 Limitations of the Study

Despite the present study finding a significant positive influence of trust on intention to adopt smart city services in regional Australian cities, limitations of the study must be acknowledged. While care has been taken during the process of exploring the research problem, developing the research model, selecting participants and research methods and analysing data to draw conclusions, there are further gaps created by the study, which opens the door for further research in the related field of smart city adoption. This study has two limitations.

Firstly, results of this quantitative study are based on the data collected from regional cities of Queensland, state of Australia, focusing on smart city services adoption in these areas. It may not be appropriate to generalise the usability of the developed model and study results to study trust-based adoption intention in all smart cities. Thus, stakeholders from a broader range of smart cities could have been included to make results more appropriate to all smart cities.

Secondly, using quantitative method only might have restricted in-depth subjective information about the significant relationships between exogenous and endogenous variables, which need to be addressed by qualitative study (Brannen, 2009). To further explore why the

relationship between variables is significant or insignificant, qualitative study should be conducted on top of this quantitative study.

7.5 Suggestions for Future Research

The study has observed that only four hypotheses are supported and there are factors such as information security culture, perceived privacy and self-efficacy in information security with positive and above 0.1 path coefficients. Those hypotheses were rejected on the basis of high p-values. This leaves the further study opportunity using these factors to test if they fit in the smart city adoption study in different locations involving different stakeholders in the sample.

Next, to conduct further study on the adoption of smart cities, the methodology could be extended to use mixed method, which uses qualitative as well as quantitative approach to discover what relationships exist between factors along with the subjective explanation for reasons behind it. Further study can be conducted by including samples from multiple types of stakeholders using mixed research methods.

7.6 Final Remarks

The current research study has developed a research framework based on the review of prior models developed for study of technology adoption and trust-based models. The data analysis using PLS-SEM validated the constructs and measurement model. The hypothesis testing showed four significant paths in the structural model depicting significant positive influence of perceived usefulness, external pressure and perceived information security on stakeholders' trust on smart city services and technologies and significant positive influence of trust on intent to adopt smart city services and technologies by its stakeholders. The results were discussed and analysed to draw conclusions. Finally, the implications of the outcomes

are discussed, and recommendations are made for future research based on the limitations of the research.

List of References

AlAwadhi, S & Morris, A 2009, 'Factors influencing the adoption of e-government services', *Journal of Software*, vol. 4*,* no.6, pp. 584-590.

Albers, S 2010, 'PLS and success factor studies in marketing', in VE Vinzi, WW Chin, J Henseler & H Wang (eds), *Handbook of partial least squares concepts, methods and applications*, pp. 409-425, Springer, Berlin Heidelberg.

Alharbi, N, Papadaki, M & Dowland, P 2017, 'The impact of security and its antecedents in behaviour intention of using e-government services', *Behaviour & Information Technology,* vol. 36**,** pp. 620-636.

AlHogail, A 2018, 'Improving IoT technology adoption through improving consumer trust', *Technologies*, vol. 6, no. 3, pp. 1-17.

AlHogail, A & AlShahrani, M 2018, 'Building consumer trust to improve internet of things (IoT) technology adoption', *Proceedings of the International Conference on Applied Human Factors and Ergonomics* pp. 325-334.

Ali, B & Awad, AI 2018, 'Cyber and physical security vulnerability assessment for IoT-based smart homes', *Sensors,* vol. 18**,** no. 3, pp. 1-17.

AlKalbani, A, Deng, H & Kam, B 2015, 'Organisational security culture and information security compliance for e-government development: the moderating effect of social pressure', *Proceedings of the Pacific Asia Conference on Information Systems (PACIS 2015)*, p. 65.

Almuraqab, NAS & Jasimuddin, SM 2017, 'Factors that influence end-users' adoption of smart government services in the UAE: a conceptual framework', *Electronic Journal of Information Systems Evaluation*, vol. 20, no*.* 1, pp. 11-23.

Alnatheer, M & Nelson, K 2009, 'Proposed framework for understanding information security culture and practices in the Saudi context', *Proceedings of the 7th Australian Information Security Management Conference***,** pp. 6-17.

Al Natheer, M, Chan, T & Nelson, K 2012, 'Understanding and measuring information security culture', *Pacific Asia Conference on Information Systems (PACIS2012).*

Al Nuaimi, E, Al Neyadi, H, Mohamed, N & Al-Jaroodi, J 2015, 'Applications of big data to smart cities', *Journal of Internet Services and Applications*, vol. 6*,* no.1, pp. 1-15.

Al-Qutayri, MA & Jeedella, JS 2010, 'Integrated wireless technologies for smart homes applications' in Al-Qutayri, M (eds), *Smart Home Systems,* IntechOpen, United Arab Emirates.

Alsaghier, H, Ford, M, Nguyen, A & Hexel, R 2011, 'Conceptualising citizen's trust in e-government: Application of Q methodology', *Leading Issues in E-Government*, vol. 7, no. 4, pp. 295-310.

Althunibat, A, Zain, NAM & Sahari, N 2011, 'The effect of social influence on mobile governmt adoption in Malaysia', *Journal of Theoretical & Applied Information Technology*, vol. 25, no. 2, pp. 103-110.

Anderson JC, & Gerbing DW 1988, 'Structural equation modelling in practice: a review and recommended two-step approach', *Psychological Bulletin*, vol. 103, no. 3, pp. 411–423.

Andreev, P, Hearty, T, Maozz, H & Pliskin, N 2009, 'Validating formative partial least squares (PLS) models: methodological review and empirical illustration', *Proceedings of the International Conference on Information Systems (ICIS, 2009),* pp. 1-17.

Andres, L 2012, *Designing and doing survey research,* Sage Publication, London.

Arboleda, N 2017, *Australian cybersecurity spending to reach $3.8 billion in 2018: Gartner*, viewed 15 October 2018, https://www.crn.com.au/news/australian-cybersecurity-spending-to-reach-38-billion-in-2018-gartner-479420.

Astrachan, CB, Patel, VK and Wanzenried, G 2014, 'A comparative study of CB-SEM and PLS-SEM for theory development in family firm research', *Journal of Family Business Strategy*, vol. 5, no. 1, pp. 116-128.

Australian Government 2016, *Smart cities plan*, viewed 15th April 2018, https://cities.infrastructure.gov.au/18190/documents/48080.

Australian Government 2017, *Smart cities and suburbs program - round 1*, viewed 10 March, 2017, https://www.business.gov.au/~/media/business/smart-cities-and-suburbs/smart-cities-and-suburbs-program-guidelines-round-one-PDF.

Australian Government 2018, *Smart cities and suburbs program - round 2*, viewed 15 October 2018, https://www.business.gov.au/-/media/Business/Smart-cities-and-suburbs/Smart-cities-and-suburbs-Grant-opportunity-guidelines-round-2-PDF.pdf?la=en&hash=3E3DE881BAD7190C824626D088FE1CAF46C23DE8.

Baig, ZA, Szewczyk, P, Valli, C, Rabadia, P, Hannay, P, Chernyshev, M, Johnstone, M, Kerai, P, Ibrahim, A & Sansurooah, K 2017, 'Future challenges for smart cities: cyber-security and digital forensics', *Digital Investigation,* vol. 22**,** pp. 3-13.

Bagozzi, RP, Yi, Y & Phillips, LW 1991, 'Assessing construct validity in organizational research' *Administrative Science Quarterly*, vol. 36, pp. 421-458.

Balte, A, Kashid, A & Patil, B 2015, 'Security issues in internet of things (IoT): a survey', *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 5*,* no. 4, pp. 450-455.

Bandura, A 1986, *Social foundations of thought and action*, Prentice-Hall, Englewood Cliffs, New Jersey.

Bartoli, A, Hernández-Serrano, J, Soriano, M, Dohler, M, Kountouris, A & Barthel, D 2011, 'Security and privacy in your smart city', *Proceedings of the Barcelona Smart Cities Congress*, vol. 292, pp. 1-6.

Becker, JM, Klein, K & Wetzels, M 2012, 'Hierarchical latent variable models in PLS-SEM: guidelines for using reflective-formative type models', *Long Range Planning*, vol. 45*,* no. 5-6, pp. 359-394.

Belanche, D, Casaló, LV & Flavián, C 2012, 'Integrating trust and personal values into the technology acceptance model: the case of e-government services adoption', *Cuadernos de Economía y Dirección de la Empresa*, vol. 15, no. 4, pp. 192-204.

Belanger, F & Hiller, JS 2006, 'A framework for e-government: privacy implications', *Business Process Management Journal,* vol. 12**,** pp. 48-60.

Bernik, I 2014, *Cybercrime and cyber warfare,* 1st edn., John Wiley & Sons, London.

Bibri, SE 2018, 'The IoT for smart sustainable cities of the future: an analytical framework for sensor-based big data applications for environmental sustainability', *Sustainable Cities and Society,* vol. 38**,** pp. 230-253.

Bollen, K & Lennox, R 1991, 'Conventional wisdom on measurement: a structural equation perspective', *Psychological Bulletin*, vol. 110, no. 2, pp. 305-314.

Bosch, P, Jongeneel, S, Rovers, V, Neumann, HM, Airaksinen, M & Huovila, A 2017, 'CITYkeys indicators for smart city projects and smart cities', *CITYkeys Report*.

Bose, R, Luo, XR & Liu, Y 2013, 'The roles of security and trust: comparing cloud computing and banking', *Procedia-Social and Behavioral Sciences*, vol. 73, pp. 30-34.

Boudreau, MC, Gefen, D & Straub, DW 2001, 'Validation in information systems research: a state-of-the-art assessment', *MIS Quarterly*, pp. 1-16.

Brace, I 2018, *Questionnaire design: how to plan, structure and write survey material for effective market research,* Kogan Page Publishers, London.

Brannen, J 2009, 'Prologue: Mixed methods for novice researchers: reflections and themes', *International Journal of Multiple Research Approaches*, vol. 3, no. 1, pp.8-12.

Braun, T, Fung, BC, Iqbal, F & Shah, B 2018, 'Security and privacy challenges in smart cities', *Sustainable Cities and Society*, vol. 39, pp. 499-507.

Bulgurcu, B, Cavusoglu, H & Benbasat, I 2010, 'Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness', *MIS Quarterly,* vol. 34**,** pp. 523-548.

Buntz, B 2017, *7 smart city strategies from cities across the world*, viewed 17 March 2018, http://www.ioti.com/smart-cities/7-smart-city-strategies-cities-across-world.

Burns, N & Grove, SK 2005, *The practice of nursing research: conduct, critique, and utilization,* 5th edn., Elsevier Saunders, St Louis.

Byrne, BM 1998, *Structural equation modelling in LISREL, PRELIS, and SIMPLIS: Basic concepts, applications, and programming*, Lawrence Erlbaum Associates Publishers,

Mahwah, New Jersey.

Byrne, BM 2013, *Structural equation modeling with Mplus: basic concepts, applications, and programming*, Routledge, New Jersey.

Caragliu, A, Del Bo, C & Nijkamp, P 2011, 'Smart cities in Europe', *Journal of Urban Technology*, vol. 18, no. 2, pp. 65-82.

Carter, L & McBride, A 2010, 'Information privacy concerns and e-government: a research agenda', *Transforming Government: People, Process and Policy*, vol. 4, no. 1, pp. 10-13.

Chang, HH & Wong, KH 2010, 'Adoption of e-procurement and participation of e-marketplace on firm performance: Trust as a moderator', *Information & Management*, vol. 47, no. 5-6, pp. 262-270.

Chang, IC, Hwang, HG, Yen, DC & Lian, JW 2006, 'Critical factors for adopting PACS in Taiwan: views of radiology department directors', *Decision Support Systems*, vol. 42, no. 2, pp.1042-1053.

Chakrabarty, S & Engels, DW 2016, 'A secure IoT architecture for Smart Cities', *13th IEEE Annual Consumer Communications & Networking Conference (CCNC 2016)*, pp. 812-813.

Chaula, JA, Yngstrom, L & Kowalski, S 2006, 'Technology as a tool for fighting poverty: How culture in the developing world affect the security of information systems'. *Fourth IEEE International Workshop on Technology for Education in Developing Countries (TEDC'06)*, pp. 66-70.

Chellappa, RK & Pavlou, PA 2002, 'Perceived information security, financial liability and consumer trust in electronic commerce transactions', *Logistics Information Management,* vol. 15**,** pp. 358-368.

Chen, L 2017, *Security management for the internet of things,* Unpublished Thesis, Master of Applied Science, University of Windsor.

Chen, W & Hirschheim, R 2004, 'A paradigmatic and methodological examination of information systems research from 1991 to 2001', *Information Systems Journal*, vol. 14, no. 3, pp. 197-235.

Chin, WW 1998, 'The partial least squares approach to structural equation modeling', *Modern Methods for Business Research*, vol. 295, no. 2, pp.295-336.

Chourabi, H, Nam, T, Walker, S, Gil-Garcia, JR, Mellouli, S, Nahon, K, Pardo, TA & Scholl, HJ 2012, 'Understanding smart cities: an integrative framework', *System Science (HICSS), 2012 45th Hawaii International Conference on System Sciences*, IEEE, pp. 2289-2297.

Churchill Jr, GA 1979, 'A paradigm for developing better measures of marketing constructs', *Journal of Marketing Research*, vol. 16, no. 1, pp. 64-73.

Chuttur, MY 2009, 'Overview of the technology acceptance model: origins, developments and future directions', *Working Papers on Information Systems*, vol. 9, no. 37, pp.9-37.

Cilliers, L & Flowerday, S 2015, 'The relationship between privacy, information security and the trustworthiness of a crowdsourcing system in a smart city', *Proceedings of the 3rd International Conference on Human Aspects of Information Security & Assurance*, pp. 243-255.

Colesca, SE 2009, 'Understanding trust in e-government', *Engineering Economics,* vol. 63**,** no. 4, pp. 7-15.

Coltman, T, Devinney, TM, Midgley, DF & Venaik, S 2008, 'Formative versus reflective measurement models: Two applications of formative measurement', *Journal of Business Research*, vol. 61, no. 12, pp. 1250-1262.

Commissioner for Privacy and Data Protection (CPDP) 2018, *Smart Cities: privacy and security*, Victoria, QLD, viewed: 12 March 2019, https://www.cpdp.vic.gov.au/images/content/pdf/privacy_week/Smart_Cities_Background_Paper.pdf

Conklin, A & White, GB 2006, 'E-government and cyber security: the role of cyber security exercises', *Proceedings of the 39th Annual Hawaii International Conference on System Sciences*, IEEE, pp. 79b-79b.

Cook, RD, & Weisberg, S 1982, *Residuals and influence in regression*, New York, Chapman & Hall.

Creswell, JW 2007, *Qualitative inquiry & research design: choosing among five approaches,* Sage Publications, Thousand Oaks, California.

Cudden, J 2018, 'How smart city technology are supporting Dublin's competitiveness', *Dublin Economic Monitor*, viewed 16 July 2018, http://www.dublineconomy.ie/2018/02/01/dublin-smart-city/.

Dahi, M, & Ezziane, Z 2015, 'Measuring e-government adoption in Abu Dhabi with technology acceptance model (TAM)', *International Journal of Electronic Governance*, vol. 7, no. 3, pp. 206-231.

Dahlberg, T, Mallat, N & Öörni, A 2003, 'Trust enhanced technology acceptance modelconsumer acceptance of mobile payment solutions: tentative evidence', *Stockholm Mobility Roundtable*, vol. 22, no. 1.

Davis, FD 1989, 'Perceived usefulness, perceived ease of use, and user acceptance of information technology', *MIS Quarterly*, vol. 13, no. 3, pp. 319-340.

Deren, L, JianJun, C & Yuan, Y 2015, 'Big data in smart cities', *Science China-Information Sciences*, vol. 58, no. 10.

Dewi, MAA, Hidayanto, AN, Purwandari, B, Kosandi, M & Budi, NFA 2018, 'Smart city readiness model based on technology-organization-environment (TOE) framework and its effect on adoption decision', *Proceedings of the Pacific Asia Conference Information System (PACIS 2018)*.

Dolnicar, S 2002, 'A review of data-driven market segmentation in tourism', *Journal of Travel & Tourism Marketing,* vol. 12**,** pp. 1-22.

Duan, X, Deng, H & Corbitt, B 2012, 'Evaluating the critical determinants for adopting e-market in Australian small-and-medium sized enterprises', *Management Research Review*, vol. 35, no.3, pp. 289-308.

Dubbeldeman, R & Ward, S 2015, *Smart cities: how rapid advances in technology are reshaping our economy and society*, Deloitte, The Netherlands, viewed 11 September 2019, https://www2.deloitte.com/content/dam/Deloitte/tr/Documents/public-sector/deloitte-nl-ps-smart-cities-report.pdf

Elmaghraby, AS & Losavio, MM 2014, 'Cyber security challenges in smart cities: safety, security and privacy', *Journal of Advanced Research,* vol. 5**,** pp. 491-497.

Ferraz, FS & Ferraz, CAG 2014, 'Smart city security issues: depicting information security issues in the role of an urban environment', *Proceedings of the 2014 IEEE/ACM 7th International Conference on Utility and Cloud Computing*, pp. 842 - 847.

Fishman, TD, & Flynn, M 2018, *Using public-private partnerships to advance smart cities*, viewed 15 November 2019, https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Public-Sector/gx-ps-public-private-partnerships-smart-cities-funding-finance.pdf

Flavián, C & Guinalíu, M 2006, 'Consumer trust, perceived security and privacy policy: three basic elements of loyalty to a web site', *Industrial Management & Data Systems*, vol. 106, no. 5, pp. 601-620.

Fornell, C & Larcker, DF 1981, 'Evaluating structural equation models with unobservable variables and measurement error', *Journal of Marketing Research*, vol. 18, no. 1, pp. 39-50.

Frost & Sullivan 2014, *Frost & Sullivan: global smart cities market to reach US$1.56 trillion by 2020*, viewed 16 July 2018, https://ww2.frost.com/news/press-releases/frost-sullivan-global-smart-cities-market-reach-us156-trillion-2020.

Gangwar, H, Date, H & Ramaswamy, R 2015, 'Understanding determinants of cloud computing adoption using an integrated TAM-TOE model', *Journal of Enterprise Information Management*, vol. 28, no. 1, pp.107-130.

Gefen, D, Karahanna, E & Straub, DW 2003, 'Trust and TAM in online shopping: an integrated model', *MIS Quarterly*, vol. 27, no.1, pp. 51-90.

Gefen, D, Straub, D & Boudreau, MC 2000, 'Structural equation modeling and regression: guidelines for research practice', *Communications of the Association for Information Systems*, vol. 4, no. 1, pp. 1-78.

George, D & Mallery, M 2003, *Using SPSS for Windows step by step: a simple guide and reference*, Allyn & Bacon, Boston.

Gharaibeh, A, Salahuddin, MA, Hussini, SJ, Khreishah, A, Khalil, I, Guizani, M & Al-Fuqaha, A 2017, 'Smart cities: a survey on data management, security, and enabling technologies', *IEEE Communications Surveys & Tutorials,* vol. 19**,** pp. 2456-2501.

Giffinger, R, Fertner, C, Kramar, H, Kalasek, R, Pichler-Milanovic, N & Meijers, E 2007, 'Smart cities ranking of European medium-sized cities', *Final Report,* Centre of Regional Science, Vienna UT, pp. 303-320.

Gold, AH, Malhotra, A & Segars, AH 2001, 'Knowledge management: an organizational capabilities perspective', *Journal of Management Information Systems*, vol. 18, no. 1, pp. 185-214.

Goldfinch, S, Gauld, R & Herbison, P 2009, 'The participation divide? political participation, trust in government, and e-government in Australia and New Zealand', *Australian Journal of Public Administration,* vol. 68**,** pp. 333-350.

Grandhi, S, Wibowo, S & Balasooriya, P 2019, 'Sec-HOTE-fit framework for assessing key security determinants in cloud computing adoption', *Proceedings of the Twenty-Third Pacific Asia Conference on Information Systems, China (PACIS 2019),* pp. 1-7.

Granzer, W, Kastner, W, Neugschwandtner, G & Praus, F 2006, 'Security in networked building automation systems', *IEEE International Workshop on Factory Communication Systems*,. IEEE, pp. 283-292.

Guba, EG & Lincoln, YS 1994, *Competing paradigms in qualitative research,* Sage, London.

Gupta, S & Xu, H 2010, 'Examining the relative influence of risk and control on intention to adopt risky technologies', *Journal of Technology Management & Innovation*, vol. 5, no. 4, pp. 22-37.

Guriting, P & Oly Ndubisi, N 2006, 'Borneo online banking: evaluating customer perceptions and behavioural intention', *Management Research News,* vol. 29**,** pp. 6-15.

Hair Jr., JF, Blake, W, Babin, B, & Tatham, R 2006, *Multivariate Data Analysis*, Prentice Hall, New Jersey.

Hair Jr, JF, Black, W, Babin, B & Anderson, R 2010, *Multivariate Data Analysis: a global perspective,* Pearson Education, London.

Hair Jr, JF, Hult, GTM, Ringle, C & Sarstedt, M 2016, *A primer on partial least squares structural equation modeling (PLS-SEM)*, Sage Publications, London.

Hameed, MA & Arachchilage, NAG 2016, 'A model for the adoption process of information system security innovations in organisations: a theoretical perspective'*, Proceedings of the 27th Australiasian Conference of Information Systems*.

Hamid, AMR, Sami, W & Sidek, MM 2017, 'Discriminant validity assessment: use of Fornell & Larcker criterion versus HTMT criterion', *Journal of Physics: Conference Series* vol. 890, no. 1, pp. 1-5.

Hara, M, Nagao, T, Hannoe, S & Nakamura, J 2016, 'New key performance indicators for a smart sustainable city', *Sustainability*, vol. 8*,* no.3, pp. 1-19.

Hasbini, MA & Martin, TP 2017, *The smart cities internet of access control, opportunities and cybersecurity challenges*, viewed 15 September 2019, https://securingsmartcities.org/wp-content/uploads/2017/09/SSC-IAC.pdf.

Hashim, KF, Tan, FB & Rashid, A 2015, 'Adult learners' intention to adopt mobile learning: a motivational perspective', *British Journal of Educational Technology*, vol. 46, no. 2, pp. 381-390.

Hathaway, RS 1995, 'Assumptions underlying quantitative and qualitative research: implications for institutional research', *Research in Higher Education,* vol. 36**,** pp. 535-562.

Hayat, P 2016, 'Smart cities: a global perspective', *India Quarterly,* vol. 72**,** pp. 177-191.

Henseler, J, Ringle, CM & Sarstedt, M 2015, 'A new criterion for assessing discriminant validity in variance-based structural equation modelling', *Journal of the Academy of Marketing Science*, vol. 43, no. 1, pp. 115-135.

Höjer, M, & Wangel, J 2015, *ICT Innovations for Sustainability*, Springer, Cham, pp. 333-349.

Holmes-Smith, P, Coote, L & Cunningham, E 2006, *Structural equation modelling: from the fundamentals to advanced topics*: *study guide*, School of Research, Evaluation and Measurement Services, Melbourne.

Huntley, V 2010, *Data security in a real-time world requires defense in depth strategy*, viewed 15 November 2018, https://www.propertycasualty360.com/2010/07/18/data-security-in-a-real-time-world-requires-defens/?slreturn=20181029050930.

Ibrahim, M, El-Zaart, A & Adams, C 2017, 'Stakeholders engagement in smart sustainable cities: a proposed model', *International Conference on Computer and Applications (ICCA),* IEEE, pp. 342-347.

IBM Corporation 2019, *IBM SPSS Statistics for Windows*, Version 26.0, Armonk, New York, IBM Corp.

Ijaz, S, Shah, MA, Khan, A & Ahmed, M 2016, 'Smart cities: A survey on security concerns', *International Journal of Advanced Computer Science and Applications,* vol. 7**,** pp. 612-625.

Ismail N, Jaffar N & Hooi TS 2013, 'Using EAO model to predict the self-employment intentions among the universities' undergraduates in Malaysia', *International Journal of Trade, Economics & Finance,* vol. 4, no. 5, pp. 282-287.

Jaafreh, AB 2018, 'The effect factors in the adoption of internet of things (IOT) technology in the SME in KSA: an empirical study', *International Review of Management and Business Research,* vol. 7, no. 1, pp. 136-148.

Jarvis, CB, MacKenzie, SB & Podsakoff, PM 2003, 'A critical review of construct indicators and measurement model misspecification in marketing and consumer research', *Journal of Consumer Research*, vol. 30, no. 2, pp. 199-218.

Jing, Q, Vasilakos, AV, Wan, J, Lu, J & Qiu, D 2014, 'Security of the internet of things: perspectives and challenges', *Wireless Networks,* vol. 20**,** no. 8, pp. 2481-2501.

Joshi, S, Saxena, S & Godbole, T 2016, 'Developing smart cities: an integrated framework', *Procedia Computer Science,* vol. 93**,** pp. 902-909.

Jöreskog, K & Sörbom, D 1984, *LISREL VI: Analysis of linear structural relations by maximum likelihood, instrumental variables and least squares methods*, User's guide*,* Department of Statistics*,* University of Uppsala, Uppsala, Sweden.

Jucevičius, R, Patašienė, I & Patašius, M 2014, 'Digital dimension of smart city: critical analysis', *Procedia-Social and Behavioral Sciences*, vol. 156, pp.146-150.

Juniper Research 2015, *Cybercrime will cost businesses over $2 trillion by 2019*, viewed 26 September 2017, https://www.juniperresearch.com/press/press-releases/cybercrime-cost-businesses-over-2trillion.

Kassim, NM 2017, 'Effect of perceived security and perceived privacy towards trust and the influence on internet banking usage among Malaysians', *International Academic Journal of Social Sciences*, vol. 4, no. 2, pp. 26-36.

Khan, Z, Pervez, Z & Ghafoor, A 2014, 'Towards cloud based smart cities data security and privacy management', *2014 IEEE/ACM 7th International Conference on Utility and Cloud Computing (UCC)*, pp. 806-811.

Khatoun, R & Zeadally, S 2016, 'Smart cities: concepts, architectures, research opportunities', *Communications of ACM*, vol. 59, no. 8, pp. 46-57.

Kickbusch I, Gleicher, D 2014, *Smart governance for health and well-being: the evidence,* World Health Organisation, Copenhagen, Denmark.

Kim, HW, Chan, HC & Gupta, S 2007, 'Value-based adoption of mobile internet: an empirical investigation', *Decision Support Systems*, vol. 43, no. 1, pp. 111-126.

Kim, GH, Trimi, S & Chung, JH 2014, 'Big-data applications in the government sector', *Communications of the ACM*, vol. 57, no. 3, pp. 78-85.

Kim, YH, Kim, DJ & Hwang, Y 2009, 'Exploring online transaction self-efficacy in trust building in B2C e-commerce', *Journal of Organizational and End User Computing (JOEUC)*, vol. 21, no. 1, pp. 37-59.

Kimberlin, CL & Winterstein, AG 2008, 'Validity and reliability of measurement instruments used in research', *American Journal of Health-System Pharmacy*, vol. 65, no. 23, pp. 2276-2284.

King, J & Awad, AI 2016, 'A distributed security mechanism for resource-constrained IoT devices', *Informatica,* vol. 40**,** no. 1, pp. 133.

Kline, E, Wilson, C, Ereshefsky, S, Tsuji, T, Schiffman, J, Pitts, S & Reeves, G 2012, 'Convergent and discriminant validity of attenuated psychosis screening tools', *Schizophrenia Research*, vol. 134, no. 1, pp. 49-53.

Knack, S & Zak, PJ 2003, 'Building trust: public policy, interpersonal trust, and economic development' *Supreme Court Economic Review*, vol. 10, pp. 91-107.

Koller, M 1988, 'Risk as a determinant of trust', *Basic and Applied Social Psychology*, vol. 9, no. 4, pp. 265-276.

Kourtit, K & Nijkamp, P 2012, 'Smart cities in the innovation age', *Innovation: The European Journal of Social Science Research,* vol. 25**,** pp. 93-95.

KPMG 2017, *Smart cities: a snapshot of Australia in 2017*, viewed 10 September 2018, https://assets.kpmg.com/content/dam/kpmg/au/pdf/2017/smart-cities-australia-snapshot-2017.pdf.

Kruger, HA & Kearney, WD 2006, 'A prototype for assessing information security awareness', *Computers & Security,* vol. 25**,** pp. 289-296.

Lai, IK, Tong, VW & Lai, DC 2011, 'Trust factors influencing the adoption of internet-based interorganizational systems', *Electronic Commerce Research and Applications*, vol. 10, no. 1, pp. 85-93.

Law, JK, Aggarwala, R & Fuchs, E 2019, *How can the private and public sectors work together to create smart cities?,* McKinsey & Company, viewed 15 November 2019, https://www.mckinsey.com/industries/capital-projects-and-infrastructure/our-insights/how-can-the-private-and-public-sectors-work-together-to-create-smart-cities

Lea, RJ 2017, *Smart cities: an overview of the technology trends driving smart cities,* viewed 13 October 2019, https://doi.org/doi.org/10.13140/RG.2.2.15303.39840

Lee, MK & Turban, E 2001, 'A trust model for consumer internet shopping', *International Journal of Electronic Commerce,* vol. 6**,** pp. 75-91.

Letaifa, SB 2015, 'How to strategize smart cities: revealing the SMART model', *Journal of Business Research*, vol. 68, no. 7, pp. 1414-1419.

Lew, YK & Sinkovics, RR 2012, 'Crossing borders and industry sectors: behavioral governance in strategic alliances and product innovation for competitive advantage', *Long Range Planning*, vol. 46, no. 1, pp. 13-38.

Lewis, BR, Templeton, GF & Byrd, TA 2005, 'A methodology for construct development in MIS research', *European Journal of Information Systems*, vol. 14, no. 4, pp. 388-400.

Lewis-Beck, MS, Bryman, A & Liao, T 2004, *The Sage encyclopedia of social science research methods*, vol. 3, Sage Thousand Oaks, California.

Lian, JW, Yen, DC & Wang, YT 2014, 'An exploratory study to understand the critical factors affecting the decision to adopt cloud computing in Taiwan hospital', *International Journal of Information Management*, vol. 34, no. 1, pp. 28-36.

Lippert, SK & Swiercz, PM 2005, 'Human resource information systems (HRIS) and technology trust', *Journal of Information Science*, vol. 31, no. 5, pp. 340-353.

Liu, C, Marchewka, JT, Lu, J & Yu, CS 2005, 'Beyond concern—a privacy-trust-behavioral intention model of electronic commerce', *Information & Management*, vol. 42, no. 2, pp. 289-304.

Loehlin, JC 1992, *Genes and environment in personality development,* Sage Publications, Inc., Thousand Oaks, California.

Lohmöller, JB 1989, 'Predictive vs. structural modeling: PLS vs. ML', *Latent Variable Path Modeling with Partial Least Squares*, Physica-Verlag, pp. 199-226.

Lombardi, P, Giordano, S, Farouh, H & Yousef, W 2012, 'Modelling the smart city performance', *Innovation: The European Journal of Social Science Research*, vol. 25, no. 2, pp. 137-149.

Ma, Q & Ratnasingam, P 2008, 'Factors affecting the objectives of information security management', *Proceedings of the 2008 International Conference on Information Resources Management,* pp. 29.

MacCallum, RC, Browne, MW & Sugawara, HM 1996, 'Power analysis and determination of sample size for covariance structure modeling', *Psychological Methods,* vol. 1**,** pp. 130.

Mathieson, K 1991, 'Predicting user intentions: comparing the technology acceptance model with the theory of planned behavior', *Information Systems Research,* vol. 2**,** pp. 173-191.

Mayer, RC, Davis, JH & Schoorman, FD 1995, 'An integrative model of organizational trust', *Academy of Management Review,* vol. 20**,** pp. 709-734.

McKnight, DH, Carter, M, Thatcher, JB & Clay, PF 2011, 'Trust in a specific technology: an investigation of its components and measures', *ACM Transactions on Management Information Systems (TMIS)*, vol. 2, no. 2, pp. 1-25.

McIlwraith, A 2006, *Information security and employee behaviour: how to reduce risk through employee education, training and awareness,* Gower Publishing Ltd., Hampshire.

Mehmood, Y, Ahmad, F, Yaqoob, I, Adnane, A, Imran, M & Guizani, S 2017, 'Internet-of-things-based smart cities: recent advances and challenges', *IEEE Communications Magazine,* vol. 55**,** pp. 16-24.

Mo, Y, Kim, TH-J, Brancik, K, Dickinson, D, Lee, H, Perrig, A & Sinopoli, B 2012, 'Cyber–physical security of a smart grid infrastructure', *Proceedings of the IEEE,* vol. 100**,** pp. 195-209.

Mohanty, SP, Choppali, U & Kougianos, E 2016, 'Everything you wanted to know about smart cities: the internet of things is the backbone', *IEEE Consumer Electronics Magazine*, vol. 5, no. 3, pp. 60-70.

Mokwetli, M & Zuva, T 2018, 'Adoption of the ICT security culture in SMMEs in the Gauteng province, South Africa', *Proceedings of the 2018 International Conference on Advances in Big Data, Computing and Data Communication Systems (icABCD).*

Monecke, A, & Leisch, F 2012, 'semPLS: Structural equation modeling using partial least squares', *Journal of Statistical Software*, vol. 48, no. 3, pp. 1-32.

Morse, JM 1991, 'Approaches to qualitative-quantitative methodological triangulation', *Nursing Research*, vol. 40, no. 2, pp. 120-123.

Mou, J, Shin, DH & Cohen, J 2017, 'Understanding trust and perceived usefulness in the consumer acceptance of an e-service: a longitudinal investigation', *Behaviour & Information Technology,* vol. 36**,** pp. 125-139.

Nam, T & Pardo, TA 2011, 'Conceptualizing smart city with dimensions of technology, people, and institutions', *Proceedings of the 12th annual international digital government research conference: digital government innovation in challenging times*, in Communications of ACM, pp. 282-291.

Neupane C, Wibowo, S, Grandhi, S, & Hossain R 2019, 'A trust based smart city adoption model for the australian regional cities: a conceptual framework', *Proceedings of the 30th Australasian Conference on Information Systems (ACIS 2019)*, 9-11 December, Fremantle, Australia, pp. 420-426.

Newman, I, Benz, CR & Ridenour, CS 1998, *Qualitative-quantitative research methodology: Exploring the interactive continuum*, Southern Illinois University Press, Carbondale and Edwardsville.

Nulty, DD 2008, 'The adequacy of response rates to online and paper surveys: what can be done?', *Assessment & Evaluation in Higher Education*, vol. 33, no. 3, pp. 301-314.

Nurse, JR, Creese, S & De Roure, D 2017, 'Security risk assessment in internet of things systems', *IT Professional,* vol. 19**,** pp. 20-26.

Ojo, A, Dzhusupova, Z & Curry, E 2015, 'Exploring the nature of the smart cities research landscape', In *Smarter as the new urban agenda*, pp. 23-47, Springer, Cham.

Orlikowski, WJ & Baroudi, JJ 1991, 'Studying information technology in organizations: research approaches and assumptions', *Information Systems Research*, vol. 2, no. 1, pp. 1-28.

Oyeyemi, GM, Bukoye, A & Akeyede, I 2015, 'Comparison of outlier detection procedures in multiple linear regressions', *American Journal of Mathematics and Statistics*, vol. 5, no. 1, pp. 37-41.

Pallant, J 2013, *SPSS survival manual*, McGraw Hill, Berkshire, England.

Paschke, JR 2009, *Adaptive IT capability and its impact on the competitiveness of firms: a dynamic capability perspective*, Unpublished PhD thesis, RMIT University.

Pavlou, PA, Tan, YH & Gefen, D 2003, 'Institutional trust and familiarity in online interorganizational relationships', *Proceedings of the European Conference on Information Systems (ICIS) Naples, Italy*.

Peng, DX & Lai, F 2012, 'Using partial least squares in operations management research: a practical guideline and summary of past research', *Journal of Operations Management*, vol. 30, no. 6, pp. 467-480.

Phillips, DC 1983, 'After the wake: postpositivistic educational thought', *Educational Researcher,* vol. 12**,** pp. 4-12.

Piro, G, Cianci, I, Grieco, LA, Boggia, G & Camarda, P 2014, 'Information centric services in smart cities', *Journal of Systems and Software*, vol. 88, pp. 169-188.

Plum, U & Stetter, R 2009, 'Pressure and trust in competitive engineering', *Proceedings of the 17th International Conference on Engineering Design (ICED 09),* vol. 9, pp. 69-80.

Polit, DF & Beck, CT 2006, 'The content validity index: Are you sure you know what's being reported? critique and recommendations', *Research in Nursing & Health*, vol. 29, no. 5, pp. 489–497.

Popescul, D & Radu LD 2016, 'Data security in smart cities: challenges and solutions' *Informatica Economica*, vol. 20, no. 1, pp. 29-38.

Ranjit, K 2011, *Research methodology,* 3rd edn, Sage Publications, London.

Ratten, V 2014, 'Behavioral intentions to adopt technological innovations: the role of trust, innovation and performance', *International Journal of Enterprise Information Systems (IJEIS)*, vol. 10, no. 3, pp. 1-12.

Rauniar, R, Rawski, G, Johnson, B & Yang, J 2013, 'Social media user satisfaction—theory development and research findings', *Journal of Internet Commerce*, vol. 12, no. 2, pp. 195-224.

Rhee, HS, Kim, C & Ryu, YU 2009, 'Self-efficacy in information security: its influence on end users' information security practice behavior', *Computers & Security,* vol. 28**,** pp. 816-826.

Ringle, CM, Sarstedt, M & Straub, D, 2012, 'A critical look at the use of PLS-SEM in MIS Quarterly', *MIS Quarterly*, vol. 36, no.1, pp. 3-14.

Ringle, CM, Wende, S & Will, A 2005, *Smartpls 2.0 (M3)*, SmartPLS, Hamburg.

Ringle, CM, Wende, S, & Becker, JM 2015, 'SmartPLS 3', Bönningstedt: SmartPLS, Viewed 15 September 2019, http://www.smartpls.com

Rogers, EM, 1995, 'Lessons for guidelines from the diffusion of innovations', *Joint Commission Journal on Quality and Patient Safety*, vol. 21 no. 7, pp. 324-328.

Roca, JC, García, JJ & de la Vega, JJ 2009, 'The importance of perceived trust, security and privacy in online trading systems', *Information Management & Computer Security*, vol. 17, no. 2, pp. 96-113.

Russell, DW 2002, 'In search of underlying dimensions: The use (and abuse) of factor analysis', *Personality and Social Psychology Bulletin*, vol. 28, no.12, pp. 1629-1646.

Salleh, KA & Janczewski, L 2016, 'Technological, organizational and environmental security and privacy issues of big data: a literature review', *Procedia Computer Science*, vol. 100, pp. 19-28.

Sarabdeen, J, Rodrigues, G & Balasubramanian, S 2014, 'E-Government users' privacy and security concerns and availability of laws in Dubai', *International Review of Law, Computers & Technology*, vol. 28, no. 3, pp. 261-276.

Saunders, M, Lewis, P & Thornhill, A 2009, *Research methods for business students,* Pearson Education Limited, Harlow, England.

Schaffers, H, Komninos, N, Pallot, M, Aguas, M, Almirall, E, Bakici, T, Barroca, J, Carter, D, Corriou, M, Fernadez, J & Hielkema, H 2012, *Smart cities as innovation ecosystems sustained by the future internet*, viewed 20 October 2019, https://hal.inria.fr/file/index/docid/769635/filename/FIREBALL-White-Paper-Final2.pdf

Schlienger, T & Teufel, S 2003, 'Analyzing information security culture: increased trust by an appropriate information security culture', *Proceedings of the 14th International Workshop on Database and Expert Systems Applications (IEEE),* pp. 405-409.

Schmidheiny, K 2012, 'Clustering in the linear model', *Short Guides to Microeconometrics-Universitaet Basel*, pp. 7-11.

Schreiber, JB, Nora, A, Stage, FK, Barlow, EA & King, J 2006, 'Reporting structural equation modeling and confirmatory factor analysis results: A review', *The Journal of Educational Research*, vol. 99, no. 6, pp. 323-338.

Schurr, PH & Ozanne, JL 1985, 'Influences on exchange processes: buyers' preconceptions of a seller's trustworthiness and bargaining toughness', *Journal of Consumer Research,* vol. 11**,** pp. 939-953.

Sekaran, U & Bougie, R 2016, *Research methods for business: a skill building approach*, John Wiley & Sons, West Sussex.

Shephard, H 2019, *Building trust in smart cities: thinking beyond cybersecurity and privacy*, viewed 5 November 2019, https://www.governmenteuropa.eu/building-trust-in-smart-cities/93728/

Shin, DH 2010, 'The effects of trust, security and privacy in social networking: A security-based approach to understand the pattern of adoption', *Interacting with Computers*, vol. 22*,* no. 5, pp. 428-438.

Siponen, M, Mahmood, MA & Pahnila, S 2014, 'Employees' adherence to information security policies: an exploratory field study', *Information & Management*, vol. 51, no. 2, pp. 217-224.

Stajkovic, AD & Luthans, F 1998, 'Self-efficacy and work-related performance: a meta-analysis', *Psychological Bulletin,* vol. 124**,** no. 2, pp. 240-261.

Straub, D, Boudreau, MC & Gefen, D 2004, 'Validation guidelines for IS positivist research' *Communications of the Association for Information Systems*, vol. 13, no. 1, pp. 380-427.

Suki, NM & Ramayah, T 2010, 'User acceptance of the e-government services in Malaysia: structural equation modelling approach', *Interdisciplinary Journal of Information, Knowledge and Management,* vol. 5**,** pp. 395-414.

Tabachnick, BG & Fidell, LS 2007, *Using multivariate statistics*, 3rd edn, Pearson, Boston.

Taherdoost, H 2018, 'Development of an adoption model to assess user acceptance of e-service technology: e-service technology acceptance model', *Behaviour & Information Technology*, vol. 37 no. 2, pp. 173-197.

Talari, S, Shafie-khah, M, Siano, P, Loia, V, Tommasetti, A & Catalão, JP 2017, 'A review of smart cities based on the internet of things concept', *Energies,* vol. 10**,** pp. 421.

Teo, TSH, Ranganathan, C & Dhaliwal, J 2006, 'Key dimensions of inhibitors for the deployment commerce', *IEEE Transactions on Engineering Management*, vol. 53, no. 3, pp. 395–411.

Thomas, DR, Lu, IRR and Cedzynski, M 2005, 'Partial least squares: a critical review and a potential alternative', *Proceedings of the Annual Conference of Administrative Sciences Association of Canada, Management Science Division, Toronto,* pp. 121-135.

Thompson, LF & Surface, EA 2007, 'Employee surveys administered online: attitudes toward the medium, nonresponse, and data representativeness', *Organizational Research Methods,* vol. 10**,** pp. 241-261.

Toft, MB, Schuitema, G & Thøgersen, J 2014, 'Responsible technology acceptance: Model development and application to consumer acceptance of Smart Grid technology', *Applied Energy*, vol. 134, pp. 392-400.

Tolbert, CJ & Mossberger, K 2006, 'The effects of e-government on trust and confidence in government', *Public Administration Review,* vol. 66**,** pp. 354-369.

Tornatzky, LG & Fleischer, M 1990, *The process of technological innovation*, Lexington Books, Lexington, MA.

Van Zoonen, L 2016, 'Privacy concerns in smart cities', *Government Information Quarterly,* vol. 33**,** pp. 472-480.

Ullman, JB 2001, *Structural equation modeling*, in Tabachnick, BG & Fidell, LS (eds), *Using multivariate statistics*, Needham Heights, Boston, Allyn & Bacon.

Urbach, N & Ahlemann, F 2010, 'Structural equation modeling in information systems research using partial least squares', *Journal of Information Technology Theory and Application*, vol. 11, no. 2, pp. 5-40.

Van Dongen, D, Claassen, L, Smid, T & Timmermans, D 2013, 'People's responses to risks of electromagnetic fields and trust in government policy: the role of perceived risk, benefits and control', *Journal of Risk Research*, vol. 16, no. 8, pp. 945-957.

Venkatesh, V, Morris, MG, Davis, GB & Davis, FD 2003, 'User acceptance of information technology: toward a unified view', *MIS Quarterly*, pp. 425-478.

Vidyasekar, AD 2013, '*Smart city market is likely to be worth a cumulative $1.565 trillion by 2020'*, viewed 10 March 2018, https://store.frost.com/strategic-opportunity-analysis-of-the-global-smart-city-market-19888.html.

Wenge, R, Zhang, X, Dave, C, Chao, L & Hao, S 2014, 'Smart city architecture: A technology guide for implementation and design challenges', *China Communications*, vol. 11, no. 3, pp. 56-69.

Wold, H 1966, 'Nonlinear estimation by iterative least squares procedures', in David, FN (Hrsg.), Festschrift for J. Neyman*: Research Papers in Statistics,* Wiley*,* London.

Workman, M, Bommer, WH & Straub, D 2008, 'Security lapses and the omission of information security measures: a threat control model and empirical test', *Computers in Human Behavior*, vol. 24, no. 6, pp. 2799-2816.

Yeh, H 2017, 'The effects of successful ICT-based smart city services: from citizens' perspectives', *Government Information Quarterly*, vol. 34, no. 3, pp. 556-565.

Yoo, SK & Kim, BY 2018, 'A decision-making model for adopting a cloud computing system', *Sustainability*, vol. 10, no. 8, pp. 1-15.

Yusof, MM, Paul, RJ & Stergioulas, LK 2006, 'Towards a framework for health information systems evaluation', Proceedings *of the 39th Annual Hawaii International Conference on System Sciences (HICSS 2006)*, IEEE.

Zanella, A, Bui, N, Castellani, A, Vangelista, L & Zorzi, M 2014, 'Internet of things for smart cities', *IEEE Internet of Things Journal*, vol. 1, no. 1, pp. 22-32.

Zhang, K, Ni, J, Yang, K, Liang, X, Ren, J & Shen, XS 2017, 'Security and privacy in smart city applications: challenges and solutions', *IEEE Communications Magazine,* vol. 55**,** pp. 122-129.

Zhang, T, Tao, D, Qu, X, Zhang, X, Lin, R & Zhang, W 2019, 'The roles of initial trust and perceived risk in public's acceptance of automated vehicles', *Transportation Research Part C: Emerging Technologies*, vol. 98, pp. 207-220.

Zissis, D & Lekkas, D 2012, 'Addressing cloud computing security issues', *Future Generation Computer Systems,* vol. 28**,** pp. 583-592

Appendices

Appendix A: Table of Item-Item Correlation Matrix

	T_PU_1	T_PU_2	T_PU_3	T_FR_1	T_FR_2	O_ISC_1	O_ISC_2	O_ISC_3	E_PEP_1	E_PEP_2	E_GP_1	E_GP_2	S_PS_1	S_PS_2	S_PS_3	S_PS_4	S_PP_1	S_PP_2	S_PP_3	S_SEIS_1	S_SEIS_2	S_SEIS_3	S_SEIS_4	S_SEIS_5	S_SEIS_6	S_SEIS_7	S_SEIS_8	TRU_1	TRU_2	TRU_3	TRU_4	INTENT_1	INTENT_2	INTENT_3
T_PU_1	1																																	
T_PU_2	.31	1																																
T_PU_3	.40	.43	1																															
T_FR_1	.20	.38	.35	1																														
T_FR_2	.207**	.390**	.313**	.608**	1																													
O_ISC_1	0.095	.287**	.200**	.292**	.353**	1																												
O_ISC_2	.331**	.266**	.218**	.292**	.340**	.439**	1																											
O_ISC_3	.248**	.287**	.211**	.376**	.419**	.565**	.600**	1																										
E_PEP_1	.332**	.347**	.456**	.289**	.216**	.275**	.456**	.287**	1																									
E_PEP_2	.349**	.381**	.467**	.314**	.328**	.254**	.442**	.284**	.509**	1																								
E_GP_1	0.119	.219**	0.096	.141*	.239**	.360**	.426**	.428**	.152*	0.129	1																							
E_GP_2	-0.051	.227**	-0.005	.139*	.268**	.372**	.379**	.473**	.189**	.160*	.401**	1																						
S_PS_1	.327**	-0.044	0.071	0.123	.294**	.233**	.350**	.378**	.168*	0.086	.321**	.216**	1																					
S_PS_2	.211**	.186**	.276**	.328**	.349**	0.041	.283**	.168*	.378**	.221**	0.055	0.117	.261**	1																				
S_PS_3	.270**	.174**	.222**	.408**	.422**	.165*	.409**	.346**	.265**	.141*	.228**	.153*	.392**	.418**	1																			
S_PS_4	.192**	.154*	.241**	.357**	.411**	.273**	.330**	.345**	.273**	.233**	0.105	.196**	.316**	.316**	.373**	1																		
S_PP_1	.226**	0.111	.139*	.256**	.134*	-0.067	0.027	-0.072	.168*	.173**	-0.061	-.177**	0.043	.255**	0.083	.231**	1																	
S_PP_2	.177**	.260**	.252**	.405**	.378**	.164*	0.131	.221**	.208**	.154*	0.029	.183**	.205**	.318**	.178**	.279**	.201**	1																	
S_PP_3	.226**	.299**	.283**	.419**	.473**	.244**	.240**	.310**	.157*	.253**	.213**	.298**	.233**	.364**	.268**	.383**	.235**	.408**	1																
S_SEIS_1	-0.052	.170*	0.107	.244**	.378**	.286**	.201**	.313**	-0.015	.174**	.169*	.292**	.151*	0.073	.141*	0.074	-0.084	.178**	.284**	1															
S_SEIS_2																																		
S_SEIS_3																																		
S_SEIS_4																																		
S_SEIS_5																																		
S_SEIS_6																																		
S_SEIS_7																																		
S_SEIS_8																																		
TRU_1																																		
TRU_2																																		
TRU_3																																		
TRU_4																																		
INTENT_1																																		
INTENT_2																																		
INTENT_3																																		

	S_SEIS_2	S_SEIS_3	S_SEIS_4	S_SEIS_5	S_SEIS_6	S_SEIS_7	S_SEIS_8	TRU_1	TRU_2	TRU_3	TRU_4	INTENT_1	INTENT_2	INTENT_3
T_PU_1	.277**	.138*	.162*	.151*	.147*	.172*	.148*	.212**	.332**	.359**	.279**	.372**	.350**	.273**
T_PU_2	.260**	.173**	.192**	.224**	.217**	.158*	.132*	.364**	.284**	.310**	.416**	.367**	.256**	0.125
T_PU_3	.202**	.160*	0.061	.157*	0.102	.138*	0.019	.324**	.292**	.389**	.268**	.409**	.292**	.224**
T_FR_1	.348**	.280**	.249**	.287**	.364**	.325**	.276**	.193**	.213**	.440**	.343**	.391**	.274**	.335**
T_FR_2	.358**	.284**	.274**	.275**	.295**	.171*	.239**	.255**	.291**	.421**	.334**	.353**	.369**	.345**
O_ISC_1	.358**	.374**	.378**	.277**	.332**	.231**	.178**	.279**	.181**	.324**	.350**	.267**	.229**	0.098
O_ISC_2	.555**	.533**	.559**	.399**	.431**	.390**	.417**	.363**	.292**	.451**	.445**	.337**	.350**	0.093
O_ISC_3	.492**	.434**	.553**	.365**	.390**	.305**	.443**	.327**	.296**	.447**	.414**	.376**	.374**	.155*
E_PEP_1	.319**	.338**	.270**	.304**	.308**	.296**	.225**	.468**	.260**	.404**	.424**	.356**	.237**	.173**
E_PEP_2	.253**	.248**	.198**	.278**	.222**	.238**	.187**	.477**	.263**	.323**	.350**	.233**	.274**	0.088
E_GP_1	.415**	.311**	.396**	.260**	.296**	.196**	.237**	.168*	.185**	.234**	.263**	.191**	.174**	-0.035
E_GP_2	.428**	.367**	.410**	.343**	.296**	.221**	.314**	.255**	.150*	.293**	.342**	0.077	.240**	-0.040
S_PS_1	.384**	.371**	.410**	.205**	.242**	.315**	.339**	.238**	.276**	.376**	.196**	.223**	.289**	.135*
S_PS_2	.227**	.226**	.165*	.167*	.247**	.328**	.311**	.291**	.360**	.387**	.291**	.193**	.258**	.284**
S_PS_3	.345**	.352**	.291**	.223**	.300**	.276**	.306**	.231**	.239**	.405**	.255**	.269**	.265**	.279**
S_PS_4	.280**	.378**	.227**	.183**	.288**	.272**	.317**	.316**	.436**	.323**	.249**	.250**	.330**	.222**
S_PP_1	0.012	0.030	-0.081	0.086	.143*	0.120	0.097	0.084	.182**	.158*	0.122	0.129	.130	.272**
S_PP_2	.278**	.270**	0.116	.237**	.275**	.281**	.271**	.232**	.234**	.361**	.185**	.353**	.389**	.192**
S_PP_3	.291**	.322**	.194**	.210**	.295**	.188**	.222**	.203**	.352**	.443**	.246**	.378**	.372**	.284**
S_SEIS_1	.215**	.134*	.258**	.303**	.195**	.032	.192**	.163*	0.021	.224**	.221**	.186**	.212**	0.056
S_SEIS_2	1	.600**	.633**	.497**	.481**	.461**	.397**	.235**	.225**	.371**	.294**	.284**	.391**	0.109
S_SEIS_3		1	.562**	.563**	.657**	.603**	.542**	.268**	.262**	.444**	.304**	.230**	.287**	0.015
S_SEIS_4			1	.507**	.491**	.417**	.559**	.259**	.215**	.404**	.326**	.190**	.246**	0.005
S_SEIS_5				1	.577**	.548**	.463**	.157*	0.121	.334**	.283**	.240**	.314**	0.097
S_SEIS_6					1	.642**	.508**	.216**	.173**	.450**	.377**	.326**	.288**	.246**
S_SEIS_7						1	.568**	.243**	.223**	.365**	.299**	.291**	.254**	0.107
S_SEIS_8							1	.262**	.250**	.317**	.299**	0.131	.267**	0.016
TRU_1								1	.367**	.358**	.407**	.300**	.200**	0.016
TRU_2									1	.482**	.329**	.344**	.323**	.225**
TRU_3										1	.537**	.471**	.361**	.279**
TRU_4											1	.344**	.281**	.143*
INTENT_1												1	.416**	.288**
INTENT_2													1	.288**
INTENT_3														1

Appendix B: Survey Questionnaire

Part I: Background Information

1. Name of your council: _____
2. What is your gender?
   ○ Male ○ Female
3. Which age group do you belong to?
   ○ 18 – 24 ○ 25 - 34 ○ 35 - 44 ○ 45 - 54 ○ 55 - 64
   ○ 65 or above
4. How many years of ICT experiences do you have?
   ○ Less than 2 years
   ○ 2 to 5 years
   ○ 5 to 10 years
   ○ More than 10 years
5. In which of the following areas does your job fit in?
   ○ Leadership
   ○ Technology
   ○ Consulting
   ○ Business process
   ○ Research and development
   ○ Education and training
   ○ Other

PART II: Perceived Usefulness

On scale from 1-5, please indicate your opinion on usefulness of smart cities.	Strongly disagree	Disagree	Neutral	Agree	Strongly agree
I believe smart city services will not create any harassment.	1	2	3	4	5
I believe the use of smart community services is convenient.	1	2	3	4	5
I believe the use of smart services gives me greater control.	1	2	3	4	5
I believe the use of smart services will improve the efficiency of obtaining services.	1	2	3	4	5

PART III: Functionality and Reliability

On scale from 1-5, please indicate your opinion on security culture and awareness of smart cities.	Strongly disagree	Disagree	Neutral	Agree	Strongly agree
I believe that councils' websites have sufficient technical capacity to ensure that the data I send will not be intercepted by hackers.	1	2	3	4	5
I believe that councils' websites have sufficient technical capacity to ensure that the data that I send cannot be modified by a third party.	1	2	3	4	5

PART IV: Information Security Culture

On scale from 1-5, please indicate your opinion on information security culture.	Strongly disagree	Disagree	Neutral	Agree	Strongly agree
I am familiar with the information security policies of my organisation.	1	2	3	4	5
I believe individual's role is important for escalating information security.	1	2	3	4	5
I am aware of the information security responsibilities.	1	2	3	4	5

PART V: Perceived External Pressure

On scale from 1-5, please indicate your opinion on privacy of smart cities.	Strongly disagree	Disagree	Neutral	Agree	Strongly agree
I believe the use of smart services is also an effective way to interact with government.	1	2	3	4	5
I believe the use of smart services will improve the efficiency of obtaining services.	1	2	3	4	5

PART VI: Government Policy

On scale from 1-5, please indicate your opinion on privacy of smart cities.	Strongly disagree	Disagree	Neutral	Agree	Strongly agree
I am aware of the potential damage to the information system by hacker threats.	1	2	3	4	5
I am aware of the risk of not following the information security policies in my organisation.	1	2	3	4	5

PART VI: Perceived Privacy

On scale from 1-5, please indicate your opinion on privacy of smart cities.	Strongly disagree	Disagree	Neutral	Agree	Strongly agree
I believe that there will be no loss of data that could result from an agency behaving opportunistically in smart city services.	1	2	3	4	5
I feel safe when I send personal information to councils.	1	2	3	4	5
I feel confident about privacy with regards to the smart city services.	1	2	3	4	5

PART VII: Perceived Information Security

On scale from 1-5, please indicate your opinion on perceived security of smart cities.	Strongly disagree	Disagree	Neutral	Agree	Strongly agree
In general, I believe smart services provided by the city council are reliable.	1	2	3	4	5
I believe the council shows concern for the privacy of its users.	1	2	3	4	5
I believe the information I provide to council websites will not be manipulated by inappropriate parties.	1	2	3	4	5
I believe that my transaction is secure while using the smart services.	1	2	3	4	5

PART VII: Self-Efficacy in Information Security

On scale from 1-5, please indicate your opinion on security of smart cities.	Strongly disagree	Disagree	Neutral	Agree	Strongly agree
I feel confident handling virus infected files.	1	2	3	4	5
I feel confident understanding terms relating to information security.	1	2	3	4	5
I feel confident learning the method to protect my information and information system.	1	2	3	4	5
I feel confident managing files in my computer.	1	2	3	4	5
I feel confident setting the Web browser to different security levels.	1	2	3	4	5
I feel confident using different programs to protect my information and information system.					
I feel confident updating security patches to the operating system.	1	2	3	4	5
I feel confident in following the 'user guide' when help is needed to protect my information and information system.	1	2	3	4	5

PART III: Trust

On scale from 1-5, please indicate your opinion on trust in smart city's services.	Strongly disagree	Disagree	Neutral	Agree	Strongly agree
Councils and other relevant authorities can be trusted to carry out online transactions faithfully.	1	2	3	4	5
I believe that legal and technological structures adequately protect me from problems on the internet.	1	2	3	4	5
I believe smart city services would provide a valuable service for residents in our city council.	1	2	3	4	5
I believe the responsible firm providing the smart city services will take full responsibility for any type of insecurity.	1	2	3	4	5

PART V: Intention to Adopt

On scale from 1-5, please indicate your opinion on privacy of smart cities.	Strongly disagree	Disagree	Neutral	Agree	Strongly agree
I have confidence in the technology used in smart city's services.	1	2	3	4	5
I am not concerned that the information I submitted online could be misused.	1	2	3	4	5
I believe the smart city services are safe to interact with for financial purposes.	1	2	3	4	5

Any comments (please specify): . . .